Titre: Title:	Gestion du contrôle et de la mobilité des services dans les réseaux de prochaine génération
Auteur: Author:	Claude-Olivier Pitt
Date:	2006
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Pitt, C.-O. (2006). Gestion du contrôle et de la mobilité des services dans les réseaux de prochaine génération [Mémoire de maîtrise, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/7906/

UNIVERSITÉ DE MONTRÉAL

GESTION DU CONTRÔLE ET DE LA MOBILITÉ DES SERVICES DANS LES RÉSEAUX DE PROCHAINE GÉNÉRATION

CLAUDE-OLIVIER PITT
DÉPARTEMENT DE GÉNIE INFORMATIQUE
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION DU DIPLÔME DE MAÎTRISE ÈS SCIENCES APPLIQUÉES
(GÉNIE INFORMATIQUE)
AOÛT 2006

Your file Votre référence
ISBN: 978-0-494-19323-5
Our file Notre référence
ISBN: 978-0-494-19323-5

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé :

GESTION DU CONTRÔLE ET DE LA MOBILITÉ DES SERVICES DANS LES RÉSEAUX DE PROCHAINE GÉNÉRATION

présenté par : Claude-Olivier Pitt
en vue de l'obtention du diplôme de : Maîtrise ès sciences appliquées
a été dûment accepté par le jury constitué de :

Mme NICOLESCU Gabriela, Doct., présidente du jury.
M. PIERRE Samuel, Ph.D., directeur de recherche et membre du jury.
M. QUINTERO Alejandro, Ph.D., membre du jury.

REMERCIEMENTS

J'aimerais tout d'abord remercier M. Samuel Pierre, mon directeur de recherche, pour m'avoir encadré adéquatement ainsi que pour ses judicieux conseils et son enseignement de très grande qualité.

À mes amis, Alexandre, Sébastien, Georges, Kamel, et Angelo, je suis reconnaissant pour votre appui.

Je dis aussi merci à tous mes collègues du LARIM pour ces échanges d'informations et ces discussions enrichissantes. Plus précisément, je remercie Stéphane pour son tutoriel LaTeX qui m'a été grandement utile pour la rédaction de ce document.

J'aimerais aussi remercier Laurent Marchand de la compagnie Ericsson pour le support technique et cognitif qu'il m'a fourni.

Il m'est aussi essentiel de souligner ma grande reconnaissance et mes remerciements les plus sincères à ma famille qui m'ont soutenus tout au long de mes études et plus particulièrement lors de ce projet.

RÉSUMÉ

Au cours des dernières années, nous avons assisté à une évolution exponentielle des réseaux cellulaires et de leurs services. Présentement, nous faisons face à des problèmes considérables que sont la lenteur d'absorption des nouvelles technologies par les architectures cellulaires actuelles, la mauvaise gestion des ressources et l'hétérogénéité des réseaux tant cellulaires que fixes. Pour contrer ces problèmes, plusieurs organismes ont ébauché des spécifications pour une nouvelle génération de réseaux (NGN - *Next Generation Networks*).

Dans ce projet, nous proposons une architecture ainsi que des protocoles pour améliorer la gestion et la mobilité des services de l'usager. L'architecture NGN de base, que nous avons fait évoluer, est celle du groupe TISPAN de l'ETSI. Cette architecture a été choisie pour son développement actif et rapide. D'ailleurs, les standards du TISPAN seront, avec de fortes probabilités, parmi ceux réellement implémentés.

Nous sommes les premiers à proposer des protocoles qui permettent aux opérateurs de gérer les services, les ressources et la facturation d'un de ses usagers, même s'il n'utilise pas le réseau d'accès de son opérateur (itinérance). Cela peut être ou non dans un modèle d'affaire de type MVNO (*Mobile Virtual Network Operator*). Nous entendons par gestion, que l'opérateur peut restreindre l'accès à certains services ou bien effectuer plusieurs actions pré configurées comme l'enregistrement de conversations, le filtrage et/ou la facturation par contenu. Du côté du client, lorsqu'il est en itinérance, les protocoles lui permettent une accessibilité aux mêmes services que lorsqu'il est connecté à son réseau d'attache, et ce, avec une QdS comparable. Nos protocoles affectent principalement deux sous-systèmes de l'architecture TISPAN. Le sous-système le plus touché est le RACS (*Resource and Admission Control Subsystem*) qui sert au contrôle d'admission et des réservations de ressources. Nous effleurons aussi le NASS (*Network Attachment Subsystem*) qui sert à configurer l'accès au réseau de l'usager. Les nouvelles fonctionnalités sont réparties sur trois noeuds du RACS. Premièrement, le BES (*Border Edge Site*) englobe entre-autres les fonctionnalités du BGF (*Border Gateway Function*), du MAP (*Mobility Anchor Point*) provenant du protocole HMIPV6 (*Hierarchical Mobile Internet Protocol Version 6*) et d'un NAPT (*Network Address and Port Translation*). Deuxièmement,

le AES (*Access Edge Site*) correspond à l'*Access Router*. Troisièmement, un nouveau noeud, le RACF (*Resource and Admission Control Function*) enregistre l'état de chacun des usagers dans son réseau et de ses usagers d'attache en visite d'en d'autres réseaux. Nous avons aussi créé des protocoles pour rendre les différentes fonctionnalités de la nouvelle architecture possibles. Plus précisément, nous avons créé un protocole pour gérer la synchronisation des profils lorsqu'un nouvel usager arrive dans le réseau ou se déplace dans un autre réseau. Nous en avons aussi créé un qui permet de gérer les réservations de ressources engendrées par les applications des usagers intra et inter-domaines avec ou sans IMS (*IP Multimedia Subsystem*) et même, optionnellement, avec l'utilisation d'un serveur d'applications local au réseau visité. De plus, nous avons créé un protocole de mise à jour des réservations d'un usager qui peut être engendré, entre-autre, par la modification du profil de l'usager dans son réseau d'attache. Enfin, nous avons créé un protocole qui permet de regrouper et de transmettre les informations de facturation intra et inter-domaines. Aussi, nous avons dû modifier le profil réseau du TISPAN en le divisant en deux parties : une pour l'accès et l'autre pour la QdS et le contrôle des services afin de pouvoir utiliser adéquatement nos nouveaux protocoles. Nous y avons ensuite ajouté des informations étendues par type de flot pour pouvoir rendre les profils plus portables et compatibles entre les domaines. Pour terminer, nous avons ajouté des options de contrôle des services qui permettent entre-autres à l'opérateur de bloquer ou de rediriger vers le réseau d'attache les flots ou les applications d'un usager.

Nous avons utilisé plusieurs outils pour valider notre travail. Pour commencer, nous avons fait l'étude des délais supplémentaires engendrés par l'ajout des informations dans les profils. Pour continuer, nous avons créé plusieurs modèles analytiques pour évaluer les coûts des différents protocoles. Nous avons terminé par des validations formelles des différents protocoles avec l'outil UPPAAL.

L'étude des délais supplémentaires a prouvé que l'augmentation des délais reste acceptable compte-tenu de l'ajout des nombreuses fonctionnalités. L'analyse des modèles analytiques a donné des résultats corrélés. En réalité, les délais supplémentaires sont non-négligeables, mais ils restent acceptables pour la synchronisation des profils, la réservation des ressources et l'échange des informations de facturation. De plus, les validations formelles des protocoles permettent d'affirmer qu'ils pourraient adéquatement être utilisés pour effectuer la gestion de la mobilité des services dans les NGN.

ABSTRACT

In the past years, we assisted to an exponential growth of cellular networks and services. Today, cellular operators face more and more problems, some of them are: slow absorption of new technology by actual cellular architectures, none optimal (far from it) use of physical resources and the duality of heterogeneous fixed and mobile networks. To solve these problems, some standardization bodies try to create standards for a new generation of networks (NGN - *Next Generation Networks*).

In this project, we propose an architecture and some protocols to improve users services management and mobility. The basic architecture that we improve came from the TISPAN standards. This architecture was chosen for its fast and very active development by the scientific community. According to a lot of sources, the TISPAN standards will be, with a high degree of probability, part of the real NGN implementation.

We are the first to propose some protocols that allow operators to manage services, resources and billing when the user is roaming from a different network operator, being MVNO (*Mobile Virtual Network Operator*) business model or not. Here, management includes options such as services and applications restriction, or pre-configured options like conversation tapping, filtering and content billing.

On the client side, when he is away from home, the protocols allow him to access the same services as if he was at home with a comparable QoS. Our protocols principally affect two subsystems of the TISPAN architecture. The first one is the RACS (*Resource and Admission Control Subsystem*) subsystem that manages admission control and resources reservations. The second is the NASS (*Network Attachment Subsystem*) subsystem that configures user access to the network.

New functionalities introduced are mainly separated between three RACS nodes. The first node is the BES (*Border Edge Site*) that includes: BGF (*Border Gateway Function*) functionalities, MAP (*Mobility Anchor Point*) coming from the HMIPV6 protocol (*Hierarchical Mobile Internet Protocol Version 6*) functionalities, NAPT (*Network Address and Port Translation*) functionalities and many other functionnalities. The second node is the AES (*Access Edge Site*) and it's a *Access Router* equivalent. The third and new node is the RACF (*Resource and Admission Control Function*) that stores current localisation and reservations of users in their home

domain and for those roaming to other networks.

We also create new protocols to allow these new functionalities to operate in the modified architecture. More precisely, we create a protocol for profile synchronisation when a new user arrives in a network or moves to another one. We create a second protocol that allows managing resources reservations for users' applications request in the local domain or inter-domains with or without the use of IMS (*IP Multimedia Subsystem*) and also, optionally, with the use of an applications server directly in the visited network. We also create a third protocol for reservations update of a user when he has its profile modified in its home network. Finally, we create a forth protocol for merging and transporting users' billing information intra and inter-domains. We have to modify the network original TISPAN profile by dividing it in two parts: one for the access and another one for both QoS and services control. This modification was mandatory to adequately introduce our new protocols. After that, we add QoS information for each stream type to allow profiles to be more portable and compatible between domains. The last profile modification is to add options to control services. For example, an operator can block or redirect to the home network specific user streams or applications.

To validate all this, we use three different tools. The first one is a delay study, to evaluate the additional delay generated by the additional options present in the different profiles. The second one is analytical models, to evaluate the cost of the different protocols. The third one is a network simulation using the UPPAAL tool, to perform a formal validation of the different protocols.

The delay study proves that the delay stays acceptable. The analytical models gives similar results. In reality supplementary delays are not negligible but they stay in an acceptable interval for profile synchronization, resources reservation and exchange of billing information. The protocols validation prove that models are well defined. The conclusion is that our proposition can adequately provides added values to manage NGN services mobility.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES SIGLES ET ABRÉVIATIONS

3G	Third Generation mobile systems
3GPP	3rd Generation Partnership Project
A-RACF	Access-Resource and Admission Control Function
AAA	Authentification Autorisation Accounting
AAA_H	AAA Home
AAA_P	AAA Proxy
AES	Access Edge Site
AF	Application Function
AMF	Access Management Function
ANS	Announcement Server
API	Application Programming Interface
ARF	Access Relay Function
ASF	Application Server Function
ATM	Asynchronous Transfer Mode
BES	Border Edge Site
BGF	Border Gateway Function
BGCF	Breakout Gateway Control Function
BM	Bandwidth Manager
C-BGF	Core-BGF
CA	Call Agent
CCITT	Comité Consultatif International Téléphonique et Télégraphique
CDCF	Charging and Data Collection Function
CDR	Call Detail Records
CLF	Connectivity Session Location and Repository Function
CM	Cable Modem
CMS	Call Management Server
CMTS	Cable Modem Terminaison System
CNG	Customer Network Gateway
CNGCF	CNG Configuration Function

CSCF	Call Session Control Function
$CSCF_H$	CSCF Home
$CSCF_P$	CSCF Proxy
DHCP	Dynamic Host Configuration Protocol
Diffserv	Differentiated services
DLCI	Data Link Connection Identifier
DNS	Domain Name System
ETSI	European Telecommunications Standards Institute
FR	Frame Relay
GC	Gate Controller
GII	Global Information Infrastructure
GSM	Global System for Mobile communications
HA	Home Agent
HFC	Hybrid Fiber Coaxial
HMIPv6	Hierarchical Mobile Internet Protocol Version 6 (RFC4140)
HTTP	Hypertext Transfer Protocol Server
I-BGF	Interconnection-BGF
IBCF	Interconnection Border Control Function
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISUP	Integrated Services Digital Network User Part
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication standardization sector
IVR	Interactive Voice Response
IWF	Interworking Function
KDC	Key Distribution Center
L2TF	Layer 2 Terminaison Function
LARIM	LAboratoire de recherche en Réseautique et Informatique Mobile
LEA	Legal Enforcement Agency
MAP	Mobility Anchor Point
MIPv6	Mobile Internet Protocol Version 6 (RFC3775)
MG	Media Gateway
MGC	Media Gateway Controller

MGCF	Media Gateway Control Function
MGCP	Media Gateway Control Protocol
MGF	Media Gateway Function
MPLS	Multi Protocol Label Switching
MRCF	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
MSF	Multiservice Switching Forum
MTA	Multimedia Terminal Adapter
MTP	Message Transfer Part
MVNO	Mobile Virtual Network Operator
NACF	Network Access Configuration Function
NAPT	Network Address and Port Translation
NASS	Network Attachment Subsystem
NAT	Network Address Translation
NGN	Next Generation Networks
NR	Network Resources
NRC	Network Resource Control
NT	Network Topology
OSA	Open Service Access
OSS	Operational Support Systems
PDBF	Profile Data Base Function
PES	PSTN/ISDN Emulation Subsystem
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
RACS	Resource and Admission Control Subsystem
RADIUS	Remote Authentication Dial-In User Service
RCD	Resource Control Domain
RCEF	Resource Control Enforcement Function
RKS	Record Keeping Server
RM	Ressource Manager
RSVP	Ressource reSerVation Protocol
RTSP	Real Time Streaming Protocol
SBG-CE	Session Border Gateway - Customer Edge
SBG-NC	Session Border Gateway - Network Core

SBG-NE	Session Border Gateway - Network Edge
SCCP	Signaling Connection Control Part
SCD	Service Control Decision
SCTP	Stream Control Transmission Protocol
SEGF	SEcurity Gateway Function
SG	Security Gateway
SG	Signalling Gateway
SGF	Signalling Gateway Function
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
SOAP	Simple Object Access Protocol
SPAN	Services and Protocols for Advanced Networks
SMS	Short Messages Service
SPDF	Service Policy Decision Function
SS7	Signaling System number 7
QdS	Qualité de Service
TC	Traffic condiotioning
TDM	Time Division Multiplexing
TFTP	Trivial File Transfer Protocol Server
TIPHON	Telecommunications and Internet Protocol Harmonization Over Networks
TISPAN	Telecommunications and Internet Converged Services and Protocols for Advanced Networking
UAAF	User Access Authorisation Function
UE	User Equipment
UMTS	Universal Mobile Telecommunications Service
UPSF	User Profile server Function
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VoIP	Voice over IP
WG	Working Groups
xDSL	X Digital Subscriber Line
XML	Extensible Markup Language

CHAPITRE 1

INTRODUCTION

Chaque jour, le nombre d'abonnés des services de télécommunications fixes traditionnels s'effritent au profit des services de télécommunications sans fil (Quotidien, 2005). Les habitudes de vie des usagers mutent et d'ici quelques années, le nombre d'abonnés des réseaux cellulaires dépassera probablement celui des réseaux de téléphonie fixe. Le marché de la téléphonie mobile est donc en grande croissance du point de vue du nombre d'usagers. Il est difficile de déterminer s'il s'agit de la cause ou de l'effet de l'augmentation fulgurante du nombre d'usagers des dernières années, mais l'amélioration et la diversification des services proposés sont aussi en grande évolution. Chaque jour de nouveaux services les plus variés les uns que les autres sont créés. Que l'on parle de télévision sur cellulaire ou de portails personnalisés abordant tant le divertissement que l'information, nous assistons présentement à une croissance inégalée des fonctionnalités de ces réseaux. Puisque les architectures cellulaires actuelles ne permettent pas d'absorber à un rythme satisfaisant les nouvelles technologies à cause de certaines limitations intrinsèques à leurs spécifications, des organismes internationaux comme l'ITU (*International Telecommunication Union*) tentent d'ébaucher les standards pour un nouveau type d'architecture qui permettrait de surpasser les limitations actuelles. En effet, l'ITU-T (*ITU Telecommunication standardization sector*) a créé un groupe de travail pour définir les requis et le modèle général des réseaux de prochaine génération (*Next Generation Networks* - NGN). Deux documents élaborant ces recommandations ont été publiés : Y.2001, *General overview of NGN* (ITU-T, 2004b) et Y. 2011, *General principles and general reference model for next generation networks* (ITU-T, 2004a). Nous aborderons dans ce document l'aspect de gestion de la mobilité des services, c'est-à-dire la gestion des ressources, le contrôle des services et la gestion de la facturation.

Dans ce premier chapitre d'introduction, nous présentons d'abord ce que sont les NGN et leur architecture de base. Par la suite, nous exposons les éléments de la problématique. Nous précisons ensuite les objectifs de notre recherche, et pour

terminer, nous dressons le plan de ce mémoire.

1.1 Concepts et architecture de base des NGN

L'ITU-T définit le terme NGN comme suit :

> *A Next Generation Network (NGN) is a packet-based network able to provide services including Telecommunication Services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It offers unrestricted access by users to different service providers. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.*

Les points les plus importants sont : l'utilisation d'une technologie par paquets, l'indépendance envers les technologies d'accès et le support de la mobilité des services.

Après la création des spécifications de base des NGN par l'ITU-T, d'autres organismes se sont impliqués dans l'ébauche de standards pour permettre aux réseaux actuels de migrer vers les NGN. Nous nous intéresserons particulièrement aux spécifications du TISPAN (*Telecommunications and Internet Converged Services and Protocols for Advanced Networking*) de l'ETSI (*European Telecommunications Standards Institute*) qui deviennent de plus en plus les standards mondiaux, même si l'organisme à la base est plutôt européen. Le groupe a comme objectif principal de définir un réseau multi-services, multi-protocoles, multi-accès et basé sur IP en accord avec les spécifications de l'ITU-T. Un autre point intéressant est sa rapide progression. En effet, la version 1 était due pour le milieu de 2005. Cependant, dans sa première version, les NGN sont définis pour des réseaux fixes uniquement et plusieurs aspects ne sont pas traités.

Le TISPAN de l'ETSI n'est cependant pas le seul groupe dédié à la création des standards pour les réseaux de prochaine génération. En effet, il en existe plusieurs et certains d'entre-eux seront analysés dans le prochain chapitre.

La partie des NGN qui nous intéresse particulièrement dans ce mémoire est le système NRC (*Network Resource Control*) (Operax, 2005). Les principaux objectifs de ce système sont :

- d'augmenter la vitesse de déploiement des services et des applications ;

- de créer une interface standardisée entre les applications et les fonctionnalités de transport du réseau ;
- d'augmenter les revenus des opérateurs en optimisant le partage et l'allocation des ressources.

La Figure 1.1 montre un modèle de haut niveau du NRC. Le NRC sert principalement de lien entre le réseau de transport et la partie des services en fournissant aux applications une interface standardisée pour le contrôle de la QdS bout en bout. Cette interface sert aussi à cacher le détail du contrôle aux services. Le système NRC doit être multi-services, multi-vendeurs et multi-technologie.

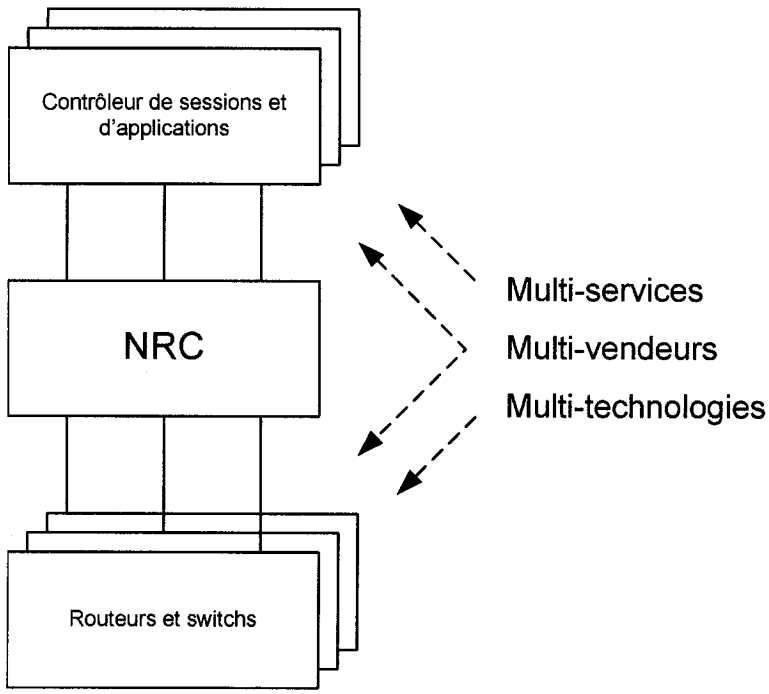

FIGURE 1.1 Modèle de haut niveau du système de contrôle des ressources

La Figure 1.2 montre l'architecture fonctionnelle du NRC. Les deux éléments principaux de ce système sont le contrôle de bande passante (*Bandwidth Control*) et le contrôle des règles (*Policy Control*). L'interface NR (*Network Resources*) sert à transmettre des requêtes de bande passante au NRC par les serveurs d'applications. Ensuite, l'interface TC (*Traffic conditioning*) sert à pousser les règles et la décision du contrôle d'admission dans les éléments du réseau (principalement le contrôle des grilles). Finalement, l'interface NT (*Network Topology*) a comme fonction la collecte des informations à propos de la topologie du réseau, de l'état des liens et

des réservations actuelles. Elle sert aussi à effectuer des réservations.

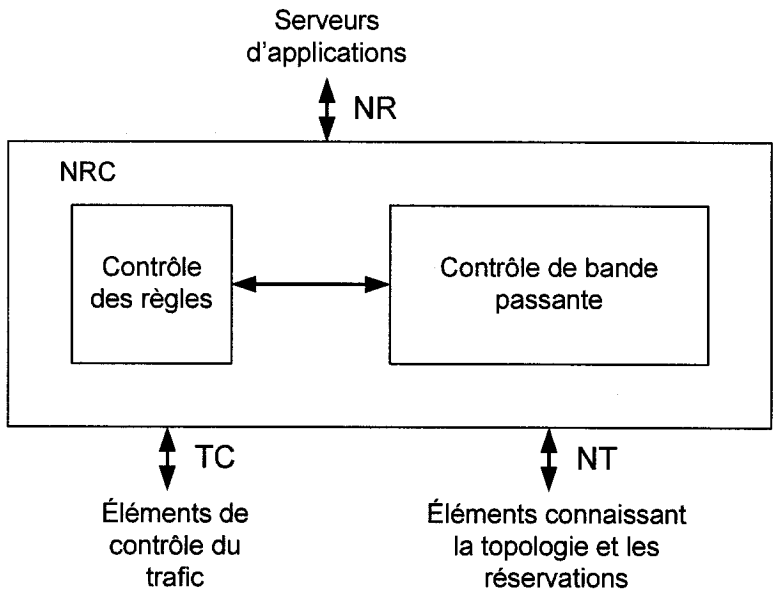

FIGURE 1.2 Modèle fonctionnel haut niveau du système de contrôle des ressources

1.2 Éléments de la problématique

Nous assistons présentement à l'explosion des réseaux mobiles et des services qui s'y rattachent. La plupart des services sont de plus en plus demandant au niveau des ressources et de la QdS (Qualité de Service). En effet, il existe une grande différence entre un SMS qui peut arriver plusieurs secondes après son envoi et l'écoute d'une émission de télévision en direct qui doit respecter certains délais et toujours rester synchronisée pour assurer une expérience adéquate à l'usager. De plus, les usagers veulent accéder à ces mêmes services en tout temps et n'importe où. Ceci entraîne plusieurs problèmes du point de vue des interconnexions inter-domaines et de la disponibilité des services, car chaque domaine doit être capable de fournir à l'usager les mêmes services avec des QdS comparables. Présentement, les architectures ne sont pas adéquates pour résoudre efficacement la majorité de ces problèmes.

L'approche logique est l'évolution vers la prochaine génération de réseaux, les NGN. Actuellement, les grandes lignes de l'architecture du TISPAN pour les NGN semblent correctement définies, mais le volet des réseaux mobiles reste à être élaboré puisque la version 1 des spécifications tient compte seulement des réseaux fixes.

Le sous-système NASS qui sert à gérer les profils des usagers est en place, mais la possibilité de gérer des profils distribués dans plusieurs domaines n'a pas encore été abordée. De plus, le sous-système RACS qui sert à réserver des ressources pour les différents services est aussi disponible, mais le mécanisme de communication inter-domaines n'est pas non plus défini. Cette option serait intéressante pour qu'un usager en visite dans un réseau puisse réserver des ressources pour ses services avec les mêmes paramètres que ceux de son profil de base. Cependant, ce profil appartient à son réseau d'attache, donc à un autre domaine. Il serait aussi utile que le domaine d'attache de l'usager puisse exercer un certain contrôle sur les ressources et les services du réseau visité afin de synchroniser les différents services de l'usager.

De plus, les opérateurs de chaque domaine aimeraient être capables d'avoir accès à un système uniforme (utilisable intra-domaine et inter-domaines) pour contrôler les services des usagers. Dans l'aspect de contrôle, on peut inclure le filtrage et tout ce qui est relié au *Legal Intercept*. Voici quelques exemples d'options qui devraient être disponibles aux fournisseurs pour gérer les services d'un client :

- blocage avec ou sans avertissement d'un (des) service(s) ;
- blocage de contenu ;
- analyse de contenu ;
- ajout d'un message ;
- duplication de flow pour analyse ou enregistrement ;
- redirection de flow ;
- blocage de flow ;
- facturation basée sur le contenu ;
- facturation basée sur le type de flow ;
- blocage ou copie d'un flot encrypté bout à bout ;
- non utilisation des routes optimales (Mobile Internet Protocol Version 6 - MIPv6 (Johnson *et al.*, 2004), Hierarchical MIPv6 - HMIPv6 (Soliman *et al.*, 2005)) ;
- introduction de gigues/délais.

Il serait aussi important de disposer d'un moyen efficace pour effectuer la facturation de l'usager même s'il n'a pas utilisé le réseau d'accès de son fournisseur d'attache.

La Figure 1.3 montre bien les quatre interfaces qui devraient exister entre le réseau d'attache d'un usager et le réseau présentement visité par celui-ci. L'interface AAA_H-AAA_P (Authentification Autorisation Accounting Home - AAA Proxy)

est utilisée pour authentifier et autoriser l'usager. L'interface MAP-HA (Mobility Anchor Point-Home Agent) est utilisée pour effectuer la mobilité IP de l'usager. L'interface $CSCF_H$-$CSCF_P$ (Call Session Control Function Home - CSCF Proxy) est utilisée pour effectuer la mobilité des applications en utilisant IMS. L'interface SERVICE n'est pas encore réglementée et c'est le but de ce mémoire. Par cette interface, le fournisseur doit être capable de contrôler les services de l'usager en accord avec son profil ainsi que les ressources nécessaires au bon fonctionnement de ces services.

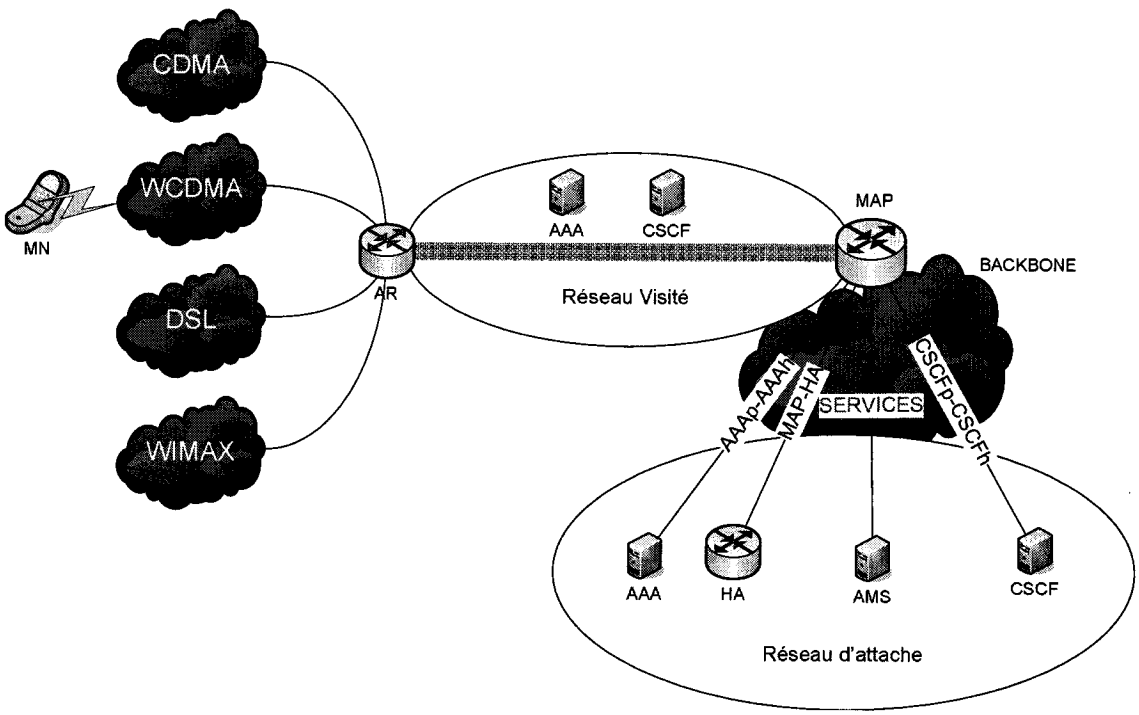

FIGURE 1.3 Problématique de l'interface SERVICE

1.3 Objectifs de recherche

L'objectif principal de ce mémoire est de concevoir un protocole efficace et évolutif, utilisable inter-domaines et intra-domaine, permettant de contrôler les ressources, les services et la facturation d'un client lorsqu'il utilise un réseau d'accès qui appartient à son fournisseur d'attache ou à un autre fournisseur. Ce protocole doit

pouvoir s'intégrer à l'architecture des NGN du TISPAN. De manière plus précise, ce mémoire vise à :

- Analyser l'architecture des NGN du TISPAN et d'autres organismes dans la perspective de leur utilisation dans les processus de gestion et de contrôle des services dans les réseaux mobiles ;
- Concevoir un protocole basé sur l'architecture des NGN du TISPAN permettant de contrôler les ressources, les services et la facturation d'un usager lorsque celui-ci utilise un réseau d'accès appartenant à son fournisseur d'attache ou à un autre fournisseur ;
- Évaluer la performance du protocole proposé à l'aide d'une validation formelle et d'un modèle analytique.

1.4 Plan du mémoire

Ce mémoire contient cinq chapitres. Après ce premier chapitre d'introduction, on retrouve le second chapitre qui explique plus amplement les sous-systèmes des NGN du TISPAN et de d'autres organismes. Plus particulièrement, nous abordons les mécanismes de réservation de ressources pour la gestion de la QdS, les mécanismes pour la gestion des profils des usagers et le système de gestion de la facturation. Le troisième chapitre décrit la solution proposée pour contrôler les ressources, les services et la facturation pour un usager qui utilise le réseau d'accès de son fournisseur d'attache ou d'un autre fournisseur ainsi que les algorithmes et le protocole qui en découlent. Le quatrième chapitre expose la validation formelle et l'évaluation de performance du protocole. Comme conclusion, le cinquième chapitre fait une synthèse des résultats obtenus, discute des limitations des travaux et indique des directions pour les recherches futures.

CHAPITRE 2

PRINCIPALES ARCHITECTURES NGN ET LEUR SYSTÈME DE RÉSERVATION DE RESSOURCES

Les NGN ont été clairement définis comme la prochaine génération de réseaux. Présentement, nous assistons à une croissance vertigineuse du nombre d'organismes qui chacun de son côté ou avec quelques interactions publie des standards. Il devient rapidement difficile de s'orienter entre ces organismes et parfois même à l'intérieur de l'un d'eux. Ce chapitre a donc comme objectif de présenter un aperçu des architectures des NGN des organismes de premier plan et plus particulièrement du système de contrôle des ressources qui effectue la gestion de la QdS. Des résumés concernant les documents techniques des principaux organismes participant au développement des NGN seront présentés dans ce chapitre. Nous aborderons tout d'abord la définition des NGN et la liste des requis fonctionnels de l'ITU-T (*International Telecommunication Union - Telecommunication standardization sector*). Ensuite, nous nous intéresserons à un joueur très important des NGN qu'est le TISPAN (*Telecommunications and Internet converged Services and Protocols for Advanced Networking*) de l'ETSI (*European Telecommunications Standards Institute*) qui incorpore le système de gestion des services du groupe 3GPP (*3rd Generation Partnership Project*). Par la suite, nous aborderons un autre organisme activement impliqué dans les NGN, le groupe MSF (*Multiservice Switching Forum*). Pour terminer, nous nous intéresserons à un dernier groupe nommé PacketCable.

2.1 ITU-T

L'ITU est le plus ancien organisme de standardisation dans le domaine des télécommunications mondiales. Il a été créé en 1865 pour faciliter l'interconnexion des réseaux de télégraphie. Aujourd'hui, il est encore l'un des organismes de premier plan dans la création des standards. L'ITU-T est l'un des trois secteurs de l'ITU.

Il a été créé en 1993, pour remplacer le *CCITT* (Comité Consultatif International Téléphonique et Télégraphique) qui datait de la création de l'ITU. La mission de L'ITU-T est de s'assurer de la qualité et de la ponctualité de la production des standards qui touchent tous les champs des télécommunications, sauf celui de la radio. Il se divise en 13 groupes de travail (*Study Groups - SG*) qui couvrent la majorité des champs d'intérêts du domaine des télécommunications. Voici une liste des principaux sujets couverts par les groupes :

- la technologie IP (*Internet Protocol*) ;
- la mobilité ;
- les technologies d'accès (principalement xDSL (*X Digital Subscriber Line*)) ;
- les réseaux optiques ;
- la gestion de la comptabilité et des tarifs ;
- les services et les systèmes multimédias.

Les prochaines sections découlent des documents suivants : (ITU-T, 2004b) et (ITU-T, 2004a).

2.1.1 Les NGN

La standardisation d'un nouveau type de réseau est maintenant devenue essentielle. Ce développement est soutenu par l'importance grandissante des éléments suivants :

- la compétition ouverte due à la déréglementation des marchés ;
- l'explosion du trafic numérique principalement dû à l'augmentation de l'utilisation d'Internet ;
- l'augmentation de la demande pour les services multimédias ;
- l'augmentation de la demande pour tous les types de mobilité ;
- la convergence des réseaux et des services.

Les NGN (*Next Generation Network*), qui sont l'implémentation concrète du GII (*Global Information Infrastructure*) (Cochennec, 2002), sont une réponse pour satisfaire ces nouvelles demandes. Les recommandations de la série *Y* de l'ITU-T ont comme objectif de fournir une base aux NGN, car les informations sur l'implémentation n'ont pas été adéquatement définies dans le GII. Le but des NGN est donc de s'assurer que tous les éléments requis pour l'interopérabilité et pour les différentes fonctionnalités du réseau supportent les applications d'une manière glo-

bale dans tous les NGN. Tout cela, en maintenant la séparation entre les fonctions de transport, de services et d'applications. Ils doivent aussi faciliter la convergence des réseaux et des services.

Voici quelques-uns des objectifs des NGN :

- promouvoir la juste compétition ;
- encourager les investissements privés ;
- définir un cadre flexible pour l'architecture ;
- permettre l'accès aux réseaux à tous.

Voici quelques caractéristiques fondamentales des NGN :

- l'utilisation des technologies par paquets ;
- la séparation entre le transport, les services et les applications ;
- les interfaces ouvertes ;
- le grand éventail de services ;
- la QdS bout-en-bout ;
- l'interconnexion avec les terminaux PSTN ;
- la mobilité générale ;
- la non-restriction d'accès aux fournisseurs pour les usagers ;
- la convergence des services entre le monde câblé et le monde sans fil ;
- l'indépendance de la technologie d'accès avec les services ;
- le support de plusieurs technologies d'accès ;
- le support des communications d'urgence ;
- l'interception légale*legal intercept.*

Les NGN doivent donner la possibilité de créer, de déployer et de contrôler une panoplie de services qui sont présentement définis ou non. Une des caractéristiques les plus importantes est la séparation des services et de la technologie de transport. Les entités fonctionnelles qui sont le contrôle des règles, des sessions, des médias, des ressources, des services et de la sécurité doivent être adéquatement distribuées dans l'architecture du réseau. L'interconnexion entre les réseaux NGN et entre les NGN et un autre type de réseau (exemple : PSTN (*Public Switched Telephone Network*), ISDN (*Integrated Services Digital Network*) ou GSM (*Global System for Mobile communications*) sera possible à l'aide de passerelles spécialisées. Les NGN supporteront différents types de terminaux variant des terminaux conçus pour les NGN aux anciens terminaux de type PSTN par exemple. Les NGN devront aussi supporter les fonctions spécialisées comme la migration des services de voix au NGN, la QdS pour

les services temps réel et la sécurité. De plus, la mobilité générale permettant des services consistants d'un réseau à l'autre et la vue d'un usager comme une entité unique, peut importe le réseau d'accès ou le terminal qu'il utilise, doit aussi être supportée.

2.1.2 Requis fonctionnels

Dans les prochaines sections plusieurs points importants des NGN seront abordés.

L'architecture

L'architecture fonctionnelle décompose les NGN en plusieurs entités et chacune doit correspondre à une seule fonction.

La QdS bout-en-bout

Les mécanismes de gestion de la QdS peuvent se diviser en deux catégories : verticale et horizontale. Les mécanismes verticaux permettent d'effectuer le lien entre les couches supérieures de gestion de QdS et celles inférieures (exemple : Diffserv (Blake *et al.*, 1998)). D'autre part, les mécanismes horizontaux permettent d'effectuer le lien entre plusieurs couches inférieures de gestion de QdS et cela est utilisé pour contrôler la QdS entre les domaines ou les réseaux. Pour tous les mécanismes, une solution bout-en-bout est recherchée.

La plate-forme des services

Les deux points les plus importants sont : la séparation entre le contrôle des services et la technologie de transport et l'extension du contrôle des services pour supporter la téléphonie et le multimédia. Tout cela, devra être effectué avec des interfaces ouvertes (*Open Interfaces*) et avec des proxys pour permettre l'interconnexion avec des tiers fournisseurs de services. Il doit aussi exister une consistance entre les services fournis à l'usager pendant son déplacement entre les réseaux. Tous les services doivent aussi être possibles entre deux usagers n'utilisant pas le même type de réseau, ni le même type de terminal.

La sécurité

Les aspects de sécurité sont étroitement liés avec l'architecture, la QdS, l'adminis-

tration du réseau, la mobilité et la facturation. Il doit donc y avoir une architecture stricte au point de vue de la sécurité. De plus, les protocoles de sécurité choisis doivent être adéquats et flexibles.

La mobilité générale

La mobilité générale permet d'utiliser plusieurs technologies d'accès à différentes localisations lorsque le terminal ou l'usager est en mouvement et d'administrer adéquatement ses applications ou ses services indépendamment des frontières des réseaux. Le mouvement entre un réseau câblé et un réseau sans fil doit aussi être supporté. L'approche doit aussi être consistante avec celle de 3G (*Third Generation mobile systems*).

L'architecture de contrôle et les protocoles

Les champs d'intérêts pour l'architecture de contrôle sont :

- les ressources et la QdS dans le réseau d'accès et dans le réseau cœur ;
- le traitement et la conversion des médias ;
- les appels et les sessions ;
- les services.

Les éléments de contrôle doivent ensuite être groupés par thèmes et ceux-ci communiqueront entre-eux avec des interfaces standardisées. Voici une liste des thèmes possibles :

- la passerelle d'accès pour médias qui comprend le contrôle du pare-feu, du NAPT (*Network Address and Port Translation*) et du point d'application des règles ;
- le contrôle des ressources qui comprend le contrôle d'admission et la gestion des demandes d'accès ;
- le contrôle des sessions qui comprend l'allocation d'adresses, la localisation de l'usager et l'administration du profil d'accès de l'usager ;
- le contrôle des services qui comprend l'enregistrement de l'usager, l'administration du profil de services de l'usager, de la gestion des requêtes de services et de l'administration de l'intégration des services.

Pour la communication des éléments de contrôle, il est possible de réutiliser des protocoles comme H.248 pour contrôler la passerelle des médias ou SIP pour contrôler les appels et les sessions.

L'architecture des services

Puisque les besoins des usagers en terme de services sont le temps réel, l'accès câblé et sans fil, la communication d'usager à usager, la communication d'usager à machine et vice-versa ; les standards doivent définir les points suivants :

- les capacités en terme de services que les NGN doivent fournir ;
- l'architecture pour les services supportant différents modèles d'affaire et la communication sans coupure dans plusieurs environnements.

Les standards doivent aussi être compatibles avec les anciennes technologies (*backward compatibility*).

L'interopérabilité des services et du réseau

Puisque les NGN impliquent un large éventail de protocoles au niveau transport et au niveau des services, il existe une certaine complexité pour l'intéropérabilité entre les services et les réseaux. Il doit donc y avoir des vérifications de compatibilité, une documentation raisonnables et des procédures adéquates.

L'adressage

Puisque les NGN sont constitués de réseaux de transport hétérogènes avec des réseaux d'accès hétérogènes et des terminaux d'usagers hétérogènes ; il existe un besoin réel et présent de définir un moyen global d'identifier les usagers. Il faut donc définir un association nom/adresse et utiliser un système pour effectuer la résolution.

La Figure 2.1 présente le modèle fonctionnel général des NGN selon la vision de l'ITU-T. Cette figure montre la relation existante entre les ressources destinées aux services et la couche service des NGN ainsi que la relation entre les ressources de transport et la couche transport des NGN.

Les fonctions de contrôle

Il existe deux types de fonctions de contrôle dans les NGN :

1. celles reliées au contrôle des services, comme l'authentification de l'usager, son identification, le contrôle d'admission pour les services et les fonctions des serveurs d'applications ;
2. celles reliées au contrôle du réseau de transport, comme le contrôle d'admission pour la connexion au réseau et le contrôle des ressources et des règles.

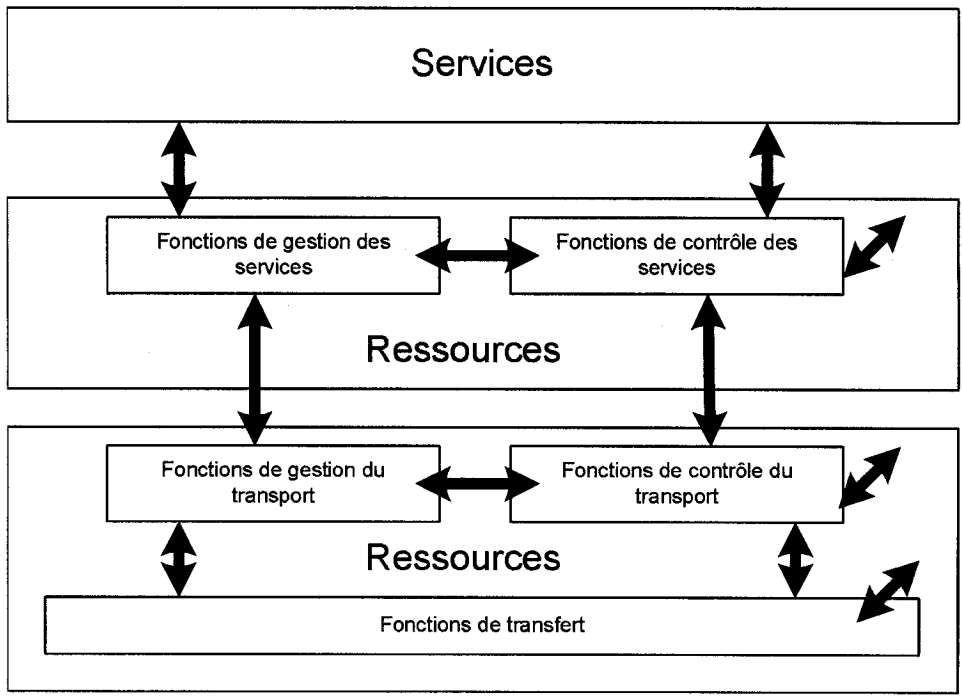

FIGURE 2.1 Modèle fonctionnel général des NGN

Les fonctions d'administration

Les fonctions d'administration comprennent les fonctions suivantes :

- la gestion des fautes ;
- la gestion de la configuration ;
- la gestion de performance ;
- la gestion de la comptabilité ;
- la gestion de la sécurité.

Les fonctions de transfert

Les fonctions de transfert doivent être séparées de celles de contrôle et d'administration. Le réseau doit être défini comme un réseau de transport des informations qui sont transférées par les fonctions de transfert.

2.2 ETSI TISPAN

Le TISPAN (*Telecommunication and Internet converged Services and Protocols for Advanced Networking*) est un groupe de l'ESTI (*European Telecommunications*

Standards Institute) qui a été créé en 2003. Il résulte de la jonction du SPAN (*Services and Protocols for Advanced Networks*), un groupe qui effectuait la définition de services et de protocoles et le TIPHON (*Telecommunications and Internet Protocol Harmonization Over Networks*), un projet créé en 1997 par l'ETSI pour étudier l'intégration de la VoIP (*Voice over IP*) et des autres multimédias sur les réseaux IP.

Le TISPAN a comme principaux centres de compétences, les réseaux fixes et la migration des réseaux à circuits commutés aux réseaux à commutation de paquets. Le but ultime est d'effectuer la convergence entres les technologies câblées, sans fil et les services de l'usager. Il est responsable de la standardisation de tous les aspects des NGN. Le TISPAN est un comité technique (*technical committee*) de l'ETSI et il est divisé en groupes de travail (*Working Groups* - WG) ayant chacun des champs de compétences distincts. Ces champs de compétences, qui correspondent chacun à un groupe de travail, sont les suivants :

1. les services (WG1) ;
2. l'architecture (WG2) ;
3. les protocoles (WG3) ;
4. le routage et les interconnexions (WG4) ;
5. la QdS (WG5) ;
6. les tests de qualité (WG6) ;
7. la sécurité (WG7) ;
8. la maintenance des standards (WG8).

Les prochaines sections découlent des documents suivants :(TISPAN, 2005a), (TISPAN, 2005b), (TISPAN, 2005c) et (TISPAN, 2005d).

L'architecture fonctionnelle des NGN du TISPAN respecte le modèle général de l'ITU-T. Elle se divise en deux parties : celle destinée aux services et celle pour le transport. Chaque partie se divise ensuite en sous-systèmes. Une approche par sous-systèmes rend le système global très évolutif. En effet, l'ajout de nouveaux sous-systèmes permet d'augmenter les fonctionnalités pour répondre à de nouvelles demandes et par conséquent à de nouveaux besoins.

La Figure 2.2 représente une vue globale de l'architecture NGN du TISPAN. Dans ce projet, nous nous intéressons principalement à la partie transport et plus précisément au sous-système RACS et légèrement au système NASS.

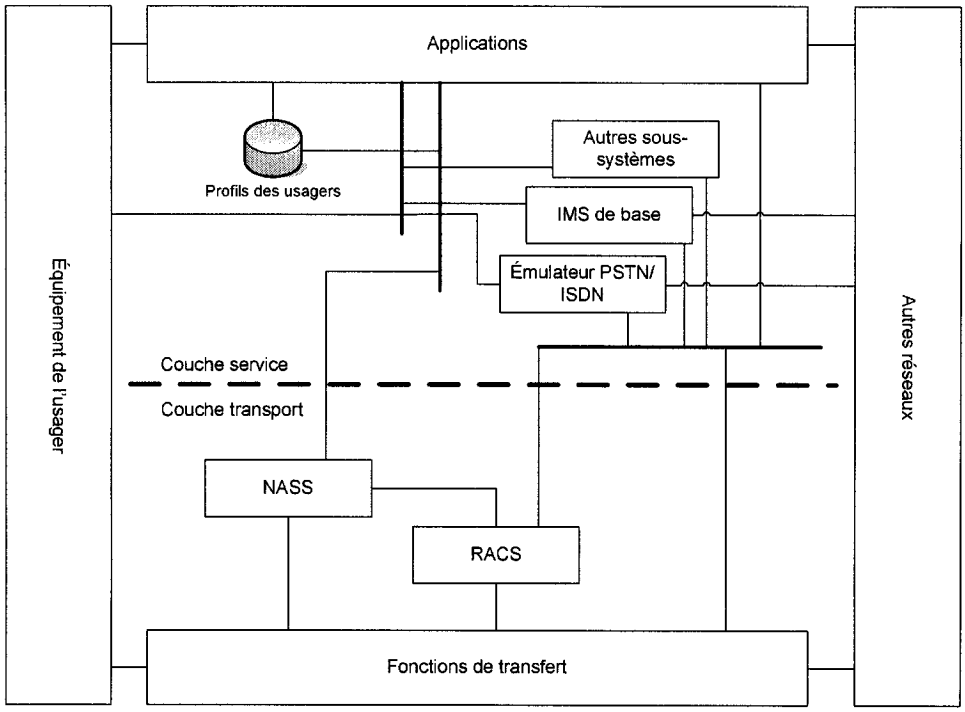

FIGURE 2.2 Architecture globale NGN du TISPAN

2.2.1 Partie services

Les différents sous-systèmes de la partie services sont les suivants :

- le *IP Multimedia Subsystem* (IMS) de 3GPP ;
- l'émulateur PSTN (*Public Switched Telephone Network*) /ISDN (*Integrated Services Digital Network*) (PSTN/ISDN Emulation Subsystem - PES) (TISPAN, 2005a) ;
- les autres sous-systèmes multimédias, comme la propagation par flot, la propagation de contenu par inondation et les applications ;
- les composantes communes, comme celles pour la facturation, pour la sécurité, pour les profils des usagers, pour accéder aux applications.

Sous-système IMS

Le sous-système IMS, présenté à la Figure 2.3, rend disponible aux usagers des services multimédias basés sur SIP. Il rend aussi accessible des services de simulation du PSTN/ISDN. Le IMS du TISPAN est une sous-partie du IMS de 3GPP ((3GPP, 2005b) et (3GPP, 2005a)). En effet, seulement les fonctionnalités de contrôle de

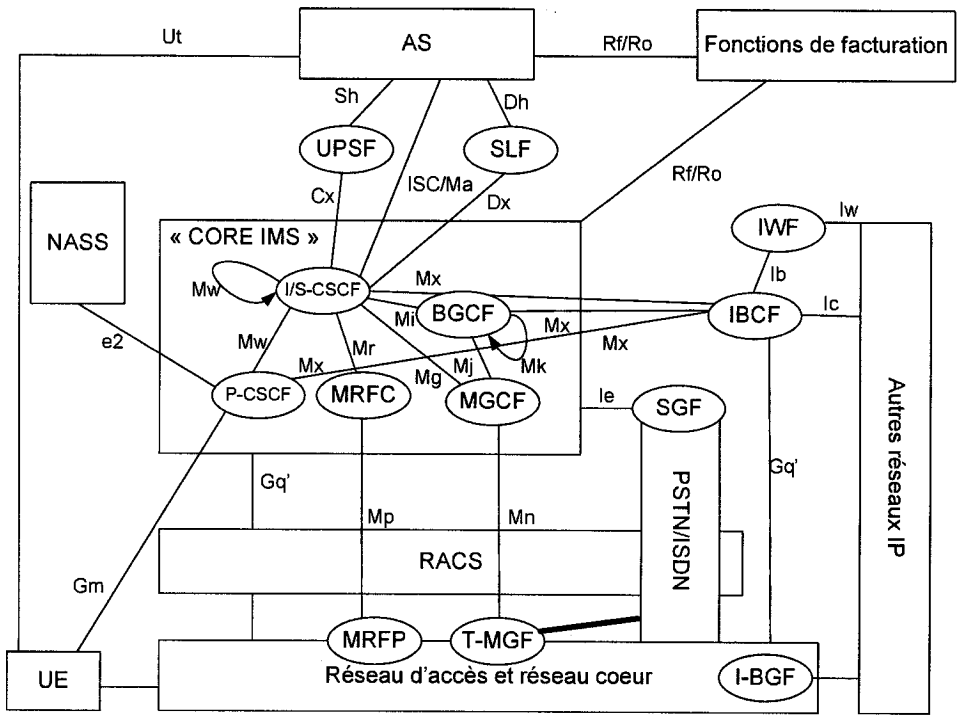

FIGURE 2.3 Architecture IMS du TISPAN

sessions y sont incluses. Les principaux éléments sont les suivants :

- le *Call Session Control Function* (CSCF) ;
- le *Media Gateway Control Function* (MGCF) ;
- le *Multimedia Resource Function Controller* (MRFC) ;
- le *Breakout Gateway Control Function* (BGCF).

Le nœud CSCF

Le CSCF établit, surveille, supporte et relâche les sessions multimédias. De plus, il s'occupe des interactions entre les différents services d'un usager. Il peut agir en trois modes :

1. procuration (*Proxy-CSCF P-CSCF*) ;
2. servant (*Serving S-CSCF*) ;
3. interrogeant (*Interrogating I-CSCF*).

Le P-CSCF est le premier point de contact de l'usager pour avoir accès au sous-système IMS. Le S-CSCF gère les sessions et leur état dans le réseau et le I-CSCF

est le point de contact dans le réseau d'un opérateur pour les connexions destinées à un abonné présent dans son réseau.

Le nœud MGCF

Le MGCF permet de contrôler le *Media Gateway Function* (MGF). Il effectue la conversion du protocole de signalisation entre SIP (*Session Initiation Protocol*) et ISUP (*Integrated Services Digital Network User Part*), qui est la partie de contrôle de l'appel dans le protocole SS7 (*Signaling System Number 7*). Il détermine aussi le prochain saut pour le routage IP, lorsque des appels sont reçus des réseaux commutés.

Le nœud MRFC

Le MRFC avec le MRFP (*Multimedia Resource Function Processor* (décrit dans la partie transport) permettent des fonctions évoluées de communication (exemple : conférences à plusieurs parties, conversions de médias). Le MRFC interprète l'information provenant du serveur d'application via le S-CSCF et contrôle le MRFP en conséquence.

Le nœud BGCF

Le BGCF détermine dans quel réseau la communication est destinée et choisit le MGCF en conséquence.

Sous-système PES

Le sous-système PES supporte l'émulation des services du PSTN/ISDN pour les anciens terminaux qui sont connectés au réseau NGN par une passerelle. Le but est de permettre aux usagers d'avoir accès aux mêmes services qu'ils recevaient préalablement du réseau PSTN et/ou ISDN.

Sous-système de propagation

Le sous-système de propagation par flots permet les services basés sur RTSP (*Real Time Streaming Protocol*). Le sous-système de propagation de contenu par inondation permet l'acheminement de masse de contenu multimédia comme les films ou les postes de télévision.

Sous-système des composantes communes

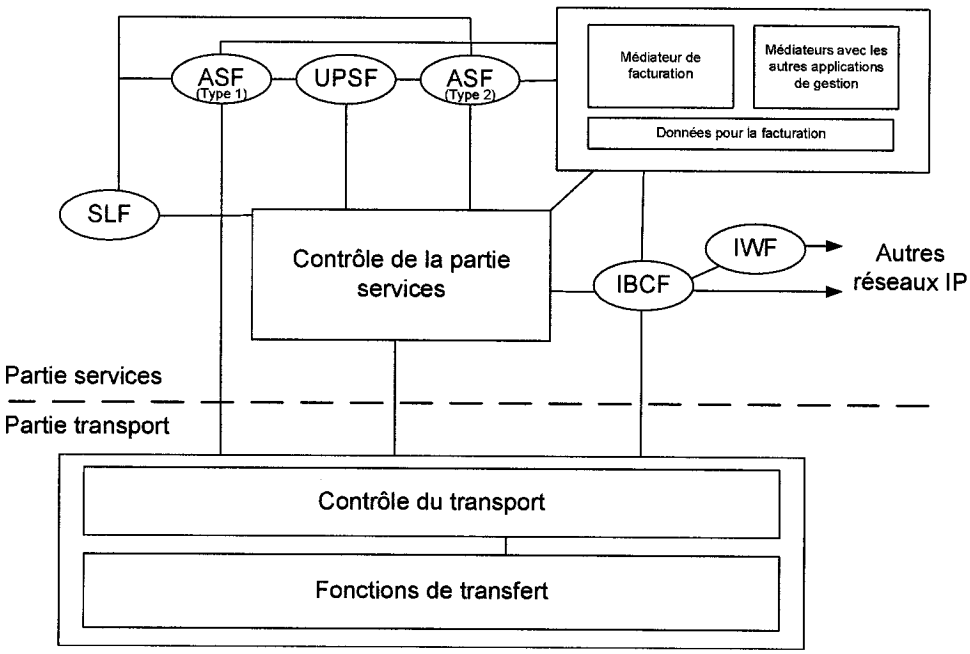

FIGURE 2.4 Composantes communes de l'architecture TISPAN

Les composantes communes (Figure 2.4) se divisent en plusieurs micro-systèmes. En voici quelques-uns :

- le *User profile server Function* (UPSF) ;
- le *Subscription Locator Function* (SLF) ;
- le *Application Server Function* (ASF) ;
- le *Interworking Function* (IWF) ;
- le *Interconnection Border Control Function* (IBCF) ;
- le *Charging and Data Collection Function* (CDCF).

Le nœud UPSF

Le UPSF contient les informations à propos des services de l'usager.

Le nœud SLF

Le SLF peut être accédé par la partie services de l'architecture TISPAN ou par le ASF pour trouver l'identité du UPSF qui contient les informations d'un usager en particulier.

Le nœud ASF

Le ASF offre des services normaux et à valeurs ajoutées. Il peut être situé dans le réseau d'attache (*home network*) de l'usager ou dans un réseau appartenant à un tier. Il existe deux types d'ASF : l'*ASF Type 1* qui communique avec le RACS pour le contrôle des ressources et l'*ASF Type 2* qui communique avec le sous-système de contrôle des services (IMS). Des exemples de ASF sont les serveurs d'applications SIP et les serveurs d'applications OSA (*Open Service Access*).

Le nœud IWF

Le IWF permet la conversion entre les différents protocoles utilisés dans le sous-système de contrôle des services (IMS) et les autres protocoles basés sur IP (par exemple entre la version de SIP utilisée dans IMS et les autres versions de SIP ou avec H.323).

Le nœud IBCF

Le IBCF permet de contrôler l'interconnexion au niveau services entre deux opérateurs (deux domaines). Il interagit avec le RACS pour avoir accès aux fonctions de NAPT et de pare-feu. De plus, il se sert du IWF lorsque le besoin de conversion est présent. Il modifie aussi les informations de signalisation pour cacher la topologie du réseau.

Le système CDCF

Le CDCF comporte les fonctions pour collecter les données et effectuer le résumé de celles-ci et les envoyer au système de facturation. Ce système supporte la facturation différée (*off-line charging*) et la facturation en temps réel (*on-line charging*).

2.2.2 Partie transport

La partie transport qui assure la connectivité IP et qui permet de masquer la technologie d'accès utilisée comporte les deux sous-systèmes suivants :

1. une sous-couche de contrôle ;
2. des fonctions de transfert.

Sous-couche de contrôle

La sous-couche de contrôle se divise en deux sous-systèmes :

1. le *Network Attachment Subsystem* (NASS) (TISPAN, 2005c) ;
2. le *Resource and Admission Control Subsystem* (RACS) (TISPAN, 2005b).

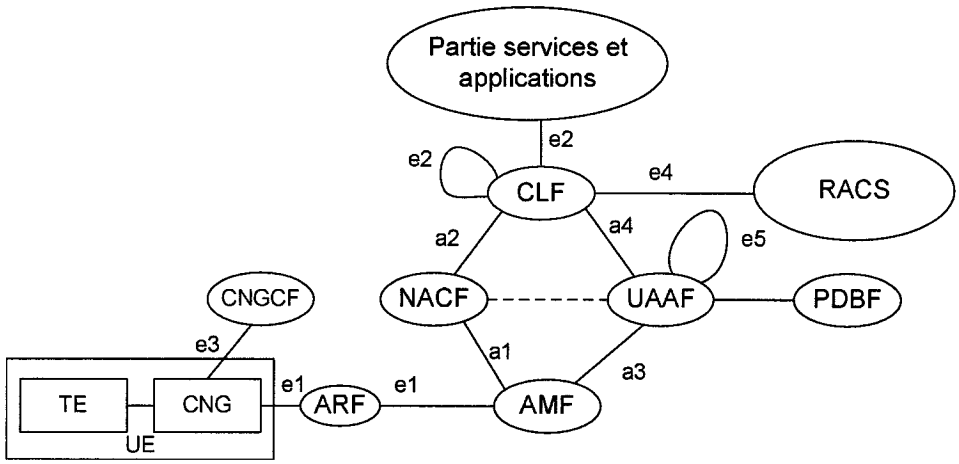

FIGURE 2.5 Architecture du NASS

Le sous-système NASS

Le sous-système NASS, présenté à la Figure 2.5, a les fonctions suivantes :

- l'attribution dynamique d'adresses IP et de paramètres de configuration aux terminaux ;
- l'authentification et l'identification de l'usager ;
- l'autorisation d'accès au réseau en fonction du profil de l'usager ;
- la configuration du réseau d'accès en fonction du profil de l'usager ;
- la localisation au niveau IP ;
- l'annonce du point de contact pour les services et les applications.

Le NASS contient les éléments fonctionnels suivants :

- le *Network Access Configuration Function* (NACF) ;
- l'*Access Management Function* (AMF) ;
- le *Connectivity Session Location and Repository Function* (CLF) ;
- le *User Access Authorisation Function* (UAAF) ;
- le *profile Data Base Function* (PDBF) ;
- le *CNG Configuration Function* (CNGCF) ;

– l'*Access Relay Function* (ARF).

Le nœud NACF

Le NACF est responsable de l'allocation d'une adresse IP et des paramètres de configuration (exemple : adresse du DNS (Domain Name System), adresse du $CSCF_P$ (*Call Session Control Function Proxy*)) à l'équipement de l'usager. Le NACF correspond donc à un serveur DHCP (*Dynamic Host Configuration Protocol*) ou RADIUS (*Remote Authentication Dial-In User Service*).

Le nœud AMF

L'AMF convertit et aiguille la requête d'accès au réseau de l'équipement de l'usager (*User Equipment - UE*). Pour ce qui concerne l'allocation de l'adresse IP et des autres paramètres de configuration, il communique avec le NACF. Pour authentifier et autoriser l'usager ainsi que pour avoir accès à des paramètres de configuration propres à celui-ci, la communication s'effectue avec le UAAF.

Le nœud CLF

Le CLF enregistre l'association entre l'adresse IP (localisation dans le réseau) de l'équipement de l'usager (UE) et sa localisation géographique (ID physique et/ou logique du réseau d'accès utilisé). Ces informations lui sont transmises par le NACF. Le CLF peut aussi mémoriser le profil de l'usager qui optionnellement peut contenir les préférences de l'usager (exemple : états des grilles) ainsi que ses options de QdS. Le profil lui est transmis par le UAAF pendant l'authentification. Ce profil servira par la suite à configurer le RACS. Plus précisément, le RACS peut demander la localisation d'un usager ainsi que son profil au CLF. Une fois le profil global de l'usager complet (informations réseau, informations géographiques, profil (comprend optionnellement les paramètres de QdS) et le profil réseau), le CLF peut répondre aux requêtes de localisation d'un usager qui proviennent de la partie des services et des applications.

Le nœud UAAF

L'UAAF effectue l'authentification et l'autorisation de l'usager en fonction de son profil. Le profil de l'usager est téléchargé du PDBF. De plus, l'UAAF collecte des données pour le service de facturation. Il peut aussi servir de proxy lorsque le

profil de l'usager se trouve dans un autre domaine ainsi que pour transmettre les informations pour le système de facturation.

Le nœud PDBF

Le PDBF contient les informations pour authentifier l'usager ainsi que son profil réseau. Le profil réseau comprend les informations pour configurer le réseau de l'usager (il est distinct du profil pour les services).

Le nœud CNGCF

Le CNGCF est utilisé pour effectuer l'initialisation ou les mises à jour de l'équipement de l'usager (exemple : pour configurer un pare-feu dans l'équipement de l'usager ou pour activer le marquage des paquets IP). Ce point de contact est particulièrement utile lorsque l'interface primaire n'est pas correctement configurée et donc inutilisable.

Le nœud ARF

L'ARF sert de relais entre le CNG (*Customer Network Gateway*) et le NASS. Ce nœud peut ajouter certains paramètres de localisation avant d'arriver au NASS.

Le sous-système RACS

Le sous-système RACS, présenté à la Figure 2.6, possède les fonctions suivantes :

- le contrôle des admissions ;
- la réservation des ressources ;
- le contrôle des politiques ;
- le contrôle des grilles (incluant le contrôle du NAPT et le marquage des priorités).

Contrôle des admissions

Le contrôle d'admission implique de vérifier l'autorisation d'un usager en fonction de son profil, des règles de l'opérateur et de la disponibilité des ressources. Pour vérifier la disponibilité des ressources, le système doit se baser sur la quantité totale de ressources que l'usager peut utiliser, de la quantité qu'il utilise présentement et de la quantité utilisée par les autres usagers. Selon ces informations, le RACS effectue ou refuse l'admission. À titre indicatif, un article (Xu et Xu, 2005) propose un mécanisme équitable de contrôle d'admission pour un réseau sans fil multimédia.

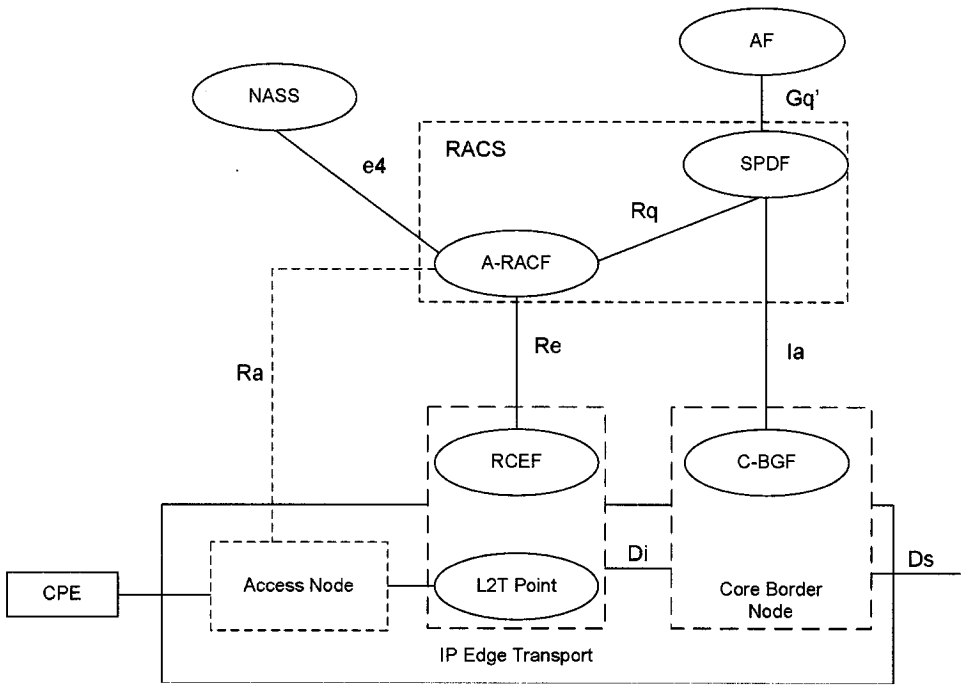

FIGURE 2.6 Architecture du RACS

Réservation des ressources

Le système fournit un mécanisme de réservation de ressources qui permet aux applications de réserver des flots de transport dans le réseau d'accès et le réseau d'agrégation.

Contrôle des politiques

Le système utilise des politiques locales basées sur les services pour savoir comment supporter chacun de ceux-ci dans la partie transport. Il vérifie ensuite les états des ressources requises pour savoir si la requête peut être autorisée. Si la réponse est positive, il autorise la requête et génère les politiques de trafic qui devront être appliquées pour supporter la session de ce service.

Contrôle des grilles

Le contrôle des grilles permet de diriger l'ouverture ou la fermeture de la barrière selon le type de service. De plus, cela permet de contrôler le NAPT.

Il est important de noter que présentement le RACS est seulement définit pour le réseau d'agrégation. En résumé, son rôle est de rendre disponible des services de

transport contrôlés par des politiques aux services et aux applications. Cela permet aux applications d'effectuer des requêtes de bande-passante à un point unique. Le RACS fonctionne par session et est donc au courant de chaque session et non de chaque application. De plus, le RACS sert à cacher la topologie du réseau de transport aux applications.

Types de QdS

Le RACS supporte trois types de QdS :

1. dynamique ;
2. statique ;
3. aucune.

Pour les types de réseaux utilisant aucune QdS et ceux dont la différentiation est configurée statiquement par les opérateurs, aucune fonctionnalité du RACS est nécessaire. Dans le cas de QdS dynamique, il existe deux types d'architectures :

1. la QdS garantie ;
2. la QdS relative.

La QdS garantie correspond à un bornage absolue sur certains ou sur tous les paramètres de QdS (exemple : bande passante, latence, jitter, perte de paquets). Pour contrôler ce type de QdS, le RACS doit effectuer du contrôle d'admission et pousser le résultat de sa décision dans le réseau d'accès au point d'entrée dans le réseau IP (*IP Edge*) ou directement dans l'équipement de l'usager ou dans le nœud d'accès (*Access Node*) sous forme de politiques de trafic. L'autre type d'architecture de QdS dynamique, celle relative, implique une différentiation (Diffserv - *Differentiated Services* (Blake *et al.*, 1998)) par classes de trafic au point d'entrée dans le réseau IP et il peut tenir compte de la capacité de certains équipements d'usager à faire de la différentiation de QdS. Les paramètres de chaque classe sont ensuite dynamiquement mis à jour. Le RACS supporte les deux types d'architectures et cela permet aux opérateurs de choisir celle qui correspond le mieux à son réseau.

Le RACS supporte aussi un autre type de mécanisme pour la réservation de ressources avec une certaine QdS. Cette dernière est utile lorsque l'application présente sur l'équipement de l'usager ne connaît pas les mécanismes de QdS. Dans ce cas-ci, l'usager demande un service au serveur d'applications (*Application Function* -

AF) et ce dernier communique avec le RACS pour la requête de QdS et pour la réservation des ressources).

Le RACS contient les éléments fonctionnels suivants :

- le *Service Policy Decision Function* (SPDF) ;
- l'*Access-Resource and Admission Control Function* (A-RACF) ;
- le *Border Gateway Function* (BGF) ;
- le *Resource Control Enforcement Function* (RCEF) ;
- le *Layer 2 Terminaison Function* (L2TF) ;
- l'*Application Function* (AF).

Le nœud SPDF

Le SPDF prend des décisions en fonction des politiques de l'opérateur. Il choisit ensuite si la requête doit être envoyée au A-RACF et/ou au BGF ainsi que les paramètres de configuration de cette/ces requête(s). Il sert aussi de point de contact unique au AF pour le système de réservation des ressources. De plus, il cache la topologie du réseau du point de vue des applications. Voici la liste plus détaillée des fonctions du SPDF :

- vérifier si la requête reçue du AF est conforme avec les politiques de l'opérateur ;
- autoriser ou refuser la requête de ressources du AF à l'aide des informations reçues ;
- déterminer la localisation du BGF et/ou du A-RACF qui peuvent accomplir la requête ;
- effectuer la demande de ressources au A-RACF ;
- effectuer la demande de services au BGF ;
- cacher le détail du système RACS et de la topologie du réseau de transport au AF ;
- effectuer l'arbitrage des ressources en mémorisant les requêtes du AF et les sous-requêtes au A-RACF et/ou au BGF.

Le nœud A-RACF

Le A-RACF a deux fonctions primaires :

1. le contrôle d'admission ;
2. l'assemblage des politiques de réseau.

Le contrôle d'admission est effectué lorsque le A-RACF reçoit une requête de réservation du SPDF. Le A-RACF utilise les paramètres de QdS transmis dans la requête pour vérifier si la ressource demandée est disponible et si elle peut fournir cette QdS. Il retourne ensuite la réponse au SPDF. Le contrôle d'admission peut aussi se produire lorsque le système NASS informe le A-RACF que usager s'est connecté au réseau. Le NASS lui transmet le profil d'accès de l'usager qui contient les informations sur son point d'attache, son profil de QdS et les configurations initiales pour les barrières. Lorsque le A-RACF a les informations du SPDF et du NASS sur un usager, il les joint ensemble. Si le profil d'accès de l'usager n'est pas reçu du NASS, la configuration locale par défaut est utilisée.

L'assemblage des politiques sert à combiner toutes les requêtes des SPDF pour s'assurer que le total des requêtes ne dépasse pas la capacité d'un certain lien d'accès (*Access Line*). Les politiques de réseau correspondent aux règles qui permettent de définir quels paramètres peuvent être appliqués à chacun des liens d'accès. Le A-RACF s'assure donc que chaque requête reçue du SPDF respecte les politiques de chacun des liens d'accès. De plus, puisque plusieurs SPDF (intra-domaine et inter-domaines) peuvent envoyer des requêtes au A-RACF, les SPDFs devraient être authentifiés et les politiques de chaque opérateur devraient être vérifiées à nouveau par le A-RACF.

Une fois le contrôle d'admission et l'assemblage des politiques effectués, en fonction des informations sur un usager et de l'état du réseau, il en dérive les règles initiales à être appliquées au RCEF. Voici une liste des mécanismes de conditionnement de trafic qui peuvent être configurés dans le RCEF à la demande du A-RACF :

- les mécanismes de niveau 2 (L2) (ex : VP/VC (*Virtual Path/ Virtual Channel*) pour ATM (*Asynchronous Transfer Mode*), DLCI (*Data Link Connection Identifier*) pour FR (*Frame Relay*), VLAN (*Virtual Local Area Network*) pour Ethernet) ;
- les mécanismes de niveau intermédiaire entre 3 et 2 (L2/L3) (ex : MPLS (*Multiprotocol Label Switching*)) ;
- les mécanismes de niveau 3 (ex : Diffserv (*Differentiated Services*) (Blake *et al.*, 1998)) ;
- les mécanismes de niveau 3 sur niveau 2 (ex : DiffServ sur ATM ou FR) ;
- les mécanismes de niveau 3 sur un niveau intermédiaire 2 et 3 (Diffserv et MPLS).

Le nœud BGF

Le BGF est une passerelle entre deux réseaux de transport par paquets. Il peut être situé à la frontière entre le réseau d'accès et l'usager, entre le réseau d'accès et le réseau cœur (C-BGF - *Core-BGF*) ou entre deux réseaux cœur (I-BGF - *Interconnection-BGF*). Il existe aussi un autre type de BGF simplifié qui est implémenté dans le réseau d'accès, le RCEF (*Resource Control Enforcement Function*). Il sera décrit dans la prochaine section. Le BGF est un point d'application des règles et peut contrôler les NAPT sous le contrôle du SPDF, et ce dans les trois parties du réseaux : l'accès, l'aggrégation et le cœur. Les principales fonctions implémentées en partie ou en totalité par les différents types de BGF sont les suivantes :

- le contrôle des services suivants : le marquage de paquet pour la QdS (par différentiation), la limitation de la bande-passante et la surveillance des taux d'utilisation ;
- la fermeture et l'ouverture de la grille en fonction des adresses IP et des services demandés ;
- la translation des adresses IP et des ports (NAPT *Network Addresses and Ports Translation*) ;
- la disponibilité des adresses et des ports pour contrôler les NAT (*Network Addresses Translation*) éloignés ;
- le disponibilité d'un ID de session indépendant de l'adresse du média ;
- le masquage la topologie du réseau ;
- le lien entre les réseau IPv4 et IPv6 ;
- l'allocation des ressources (bande-passante).

Le nœud RCEF

Le RCEF est un point d'application des règles sous le contrôle du A-RACF. Il est parfois vu comme une version simplifié de BGF. Les principales fonctions implémentées par le RCEF sont les suivantes :

- le point d'application des règles définies par l'opérateur ;
- l'ouverture ou la fermeture de la grille pour autoriser certains flots ;
- le marquage de paquets en fonction des informations reçues du A-RACF ;
- la surveillance du trafic en amont et en aval pour vérifier qu'il reste dans les limites admises.

Le nœud L2TF

Le L2TF sert de point de terminaison pour la liaison de niveau 2 (*Layer 2*) entre l'usager et le réseau d'accès.

Le nœud AF

L'AF est rarement un nœud distinct, car il est souvent inclus dans la partie services. Il sert à représenter les fonctions rendues disponibles par le RACS dans la partie services de l'architecture du TISPAN. Voici les différentes fonctionnalités que devraient implémenter ce nœud (système) :

- transmettre de l'information au SPDF à propos de la demande de QdS ;
- indiquer l'état désiré de la grille ;
- modifier ou relâcher les réservations de ressources ;
- demander les informations pour les NAT ;
- demander un *address latching.*

L'information transmise au SPDF sert à identifier le flot demandé et à quantifier la bande passante désirée. De plus, la quantité de bande passante peut être fournie comme une classe de trafic qui indique les paramètres de QdS et quels services le A-RACF et/ou le BGF doivent fournir. L'*address latching* est utilisée dans le cas où l'hébergement d'un NAT est nécessaire entre le BGF et l'usager. Ce processus correspond à déterminer l'adresse et le port utilisés par l'hôte NAT et l'enregistrer sur le BGF. Par la suite, lorsque le BGF reçoit le média pour l'usager, il le transmet à l'hôte NAT qui lui le transmet à l'usager. Tout cela, parce que l'adresse envoyée dans le paquet de signalisation correspond à l'adresse de l'usager, donc n'est pas la bonne adresse pour les communications de média (besoin de l'adresse de l'hôte NAT).

Sous-couche des fonctions de transfert

Les fonctions de transfert se répartissent dans plusieurs nœuds. Voici la liste des nœuds ayant des fonctions de transfert et qui interagissent soit avec la partie services ou la sous-couche de contrôle de la partie transport :

1. le *Border Gateway Function* (BGF) ;
2. le *Layer 2 Termination Function* (L2TF) ;
3. l'*Access Relay Function* (ARF) ;

4. le *Media Gateway Function* (MGF) ;
5. le *Media Resource Function Processor* (MRFP) ;
6. le *Signalling Gateway Function* (SGF).

Le nœud BGF

Le BGF est un nœud qui appartient à la fois au RACS et à la partie transport. Ces fonctions ont été expliquées dans la section du RACS.

Le nœud L2TF

Le L2TF est un nœud qui appartient à la fois au RACS et la partie transport. Ces fonctions ont été expliquées dans la section du RACS.

Le nœud ARF

L'ARF sert de relais entre l'usager et le sous-système NASS. Il reçoit la demande d'accès au réseau de l'usager et il la transmet au NASS. Il a été abordé dans la section du NASS.

Le nœud MGF

Le MGF permet l'attribution de média et/ou la conversion de média entre un réseau par commutation de paquets et un réseau par circuits commutés. Ce nœud effectue aussi le lien avec le sous-système d'émulation du PSTN/ISDN (PES). Il a été abordé dans la section du IMS.

Le nœud MRFP

Le MRFP supporte des fonctions spécialisées plus évoluées que celle du MGF. Parmi ses fonctions, on retrouve la conférence multimédia, l'analyse de contenu multimédia et le support de fonctions IVR (*Interactive Voice Response*). Il a été abordé dans la section IMS.

Le nœud SGF

Le dernier nœud de la partie des fonctions de transfert, le SGF, effectue la conversion dans les deux sens entre les réseau de signalisation SS7 (*Signaling System 7*) et ceux IP. Il supporte le transport de SS7 sur IP avec le protocole SCTP (*Stream Control Transmission Protocol*) et quelques fonctions de pare-feu SS7 par l'analyse

des en-têtes MTP (*Message Transfer Part*) et SCCP (*Signaling Connection Control Part*).

2.2.3 Interconnexions avec les autres réseaux

Un autre aspect important de l'architecture du TISPAN est l'interconnexion avec les autres réseaux (autres domaines). Il existe quatre niveaux d'interconnexion :

1. au niveau des fonctions de transfert ;
2. au niveau du NASS ;
3. au niveau du RACS ;
4. au niveau de la partie services.

Interconnexion au niveau des fonctions de transfert de la partie transport

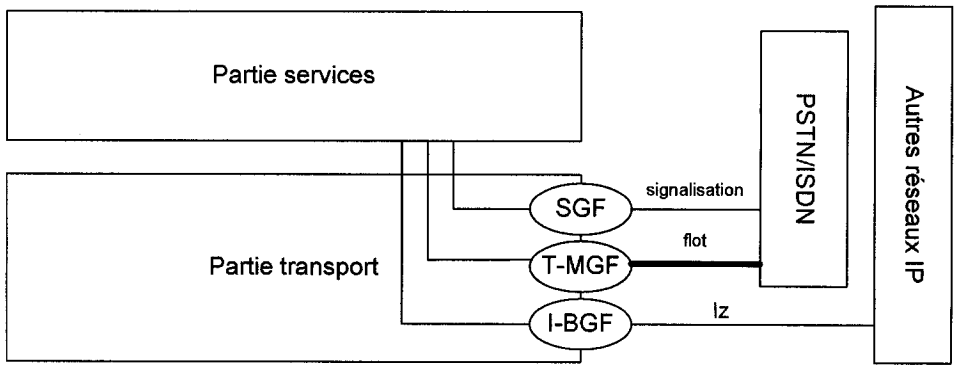

FIGURE 2.7 Interconnexion au niveau transfert

La Figure 2.7 montre les différents nœuds impliqués lors d'une interconnexion au niveau des fonctions de transfert. Lors d'une interconnexion avec un réseau TDM (*Time Division Multiplexing*), le T-MGF et le SGF sont utilisés et pour une interconnexion avec un autre réseau IP, seulement le I-BGF est utilisé. Dans ce dernier cas, le I-BGF peut être sous le contrôle du RACS, si le service implique l'IMS ou le PES. Pour ce qui est des réseaux qui utilisent la signalisation SS7, la partie service (IMS et le PES) utilise le T-MGF pour effectuer l'interconnexion.

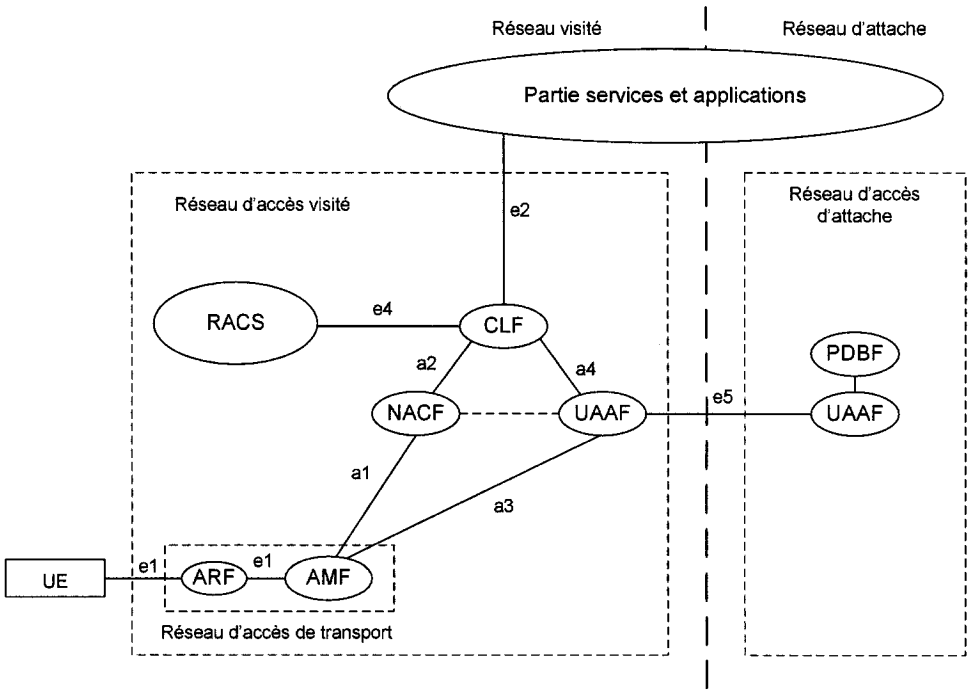

FIGURE 2.8 Interconnexion au niveau du NASS scenario 1

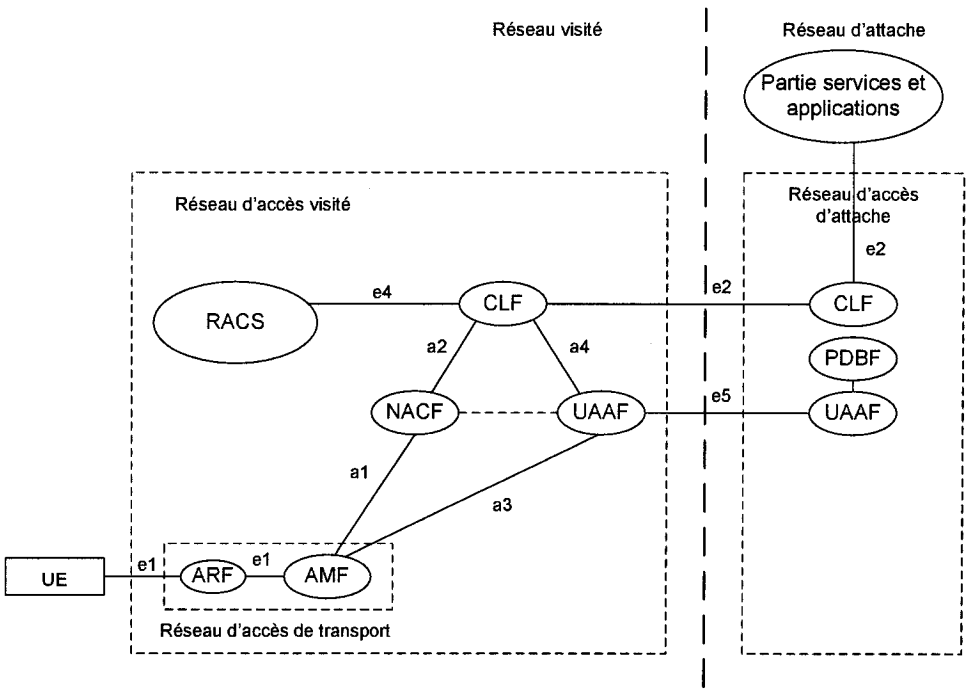

FIGURE 2.9 Interconnexion au niveau du NASS scenario 2

Interconnexion au niveau du NASS

L'interconnexion au niveau du NASS est requise pour permettre le nomadisme et l'itinérance. La Figure 2.8 montre un scénario où le profil de l'usager est téléchargé dans son réseau d'attache par le UAAF du réseau visité. De plus, la partie services est fournie par le réseau visité. Dans la Figure 2.9, le scénario est différent. En effet, la partie services est entièrement fournie par le réseau d'attache. Dans un cas pratique idéal, c'est-à-dire où tous les services que nécessite l'usager sont disponibles dans le réseau visité et qu'une entente d'itinérance existe, le scénario 1 sera utilisé.

Interconnexion au niveau du RACS

L'interconnexion au niveau du RACS n'a pas encore été abordée. Ce type d'interconnexion fait partie de la recherche courante et sera abordée plus en détail dans le prochain chapitre.

Interconnexion au niveau de la partie services

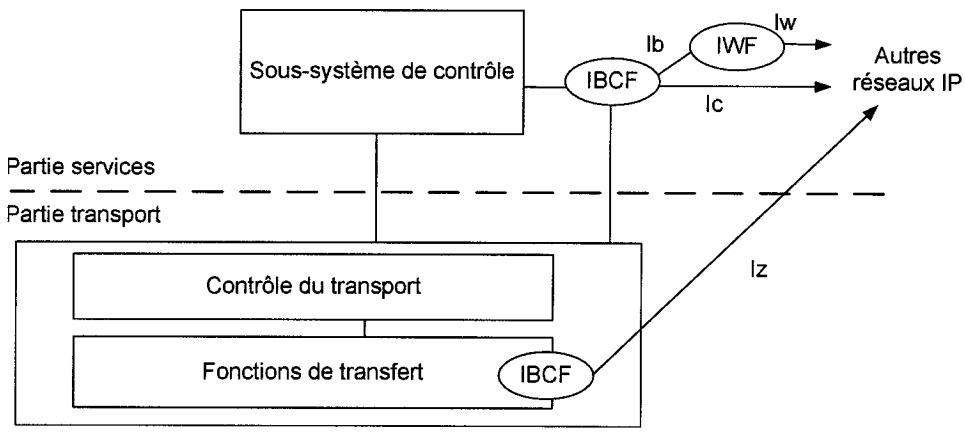

FIGURE 2.10 Interconnexion au niveau service

La Figure 2.10 montre les différents nœuds impliqués lors d'une interconnexion au niveau de la partie services. L'interconnexion avec des réseaux SS7 est contrôlée par l'IMS et le PES. Dans ce cas précis, le T-MGF et le SGF sont utilisés. L'interconnexion avec les réseaux IP dépend du type de service. Si le service utilise l'IMS ou le PES, le IBCF et possiblement le IWF (pour les conversions) seront utilisés. Si l'interconnexion est effectuée avec un réseau IP qui supporte la même version de

SIP (compatible TISPAN) seulement le IBCF est utilisé. Par contre, si le réseau ne supporte pas la même version de SIP ou supporte H.323, le IWF est aussi utilisé.

2.2.4 Connexion avec l'équipement de l'usager

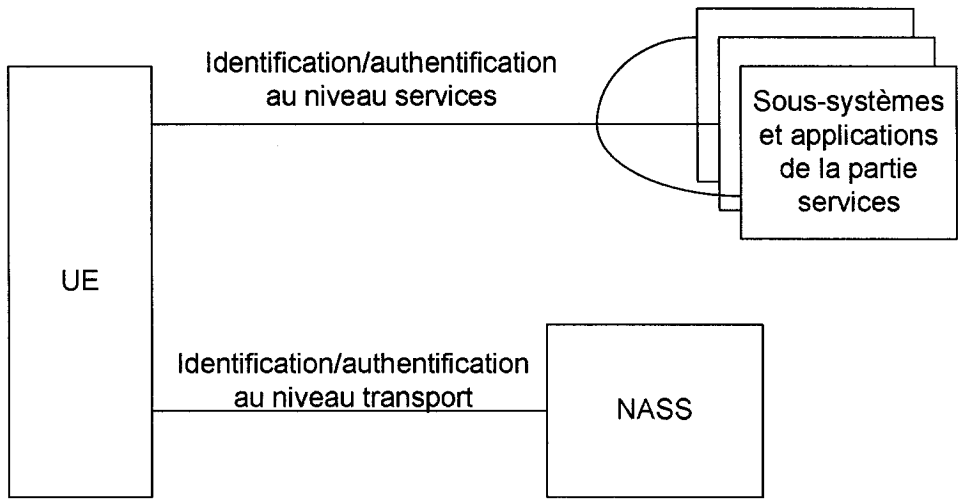

FIGURE 2.11 Connexion de l'usager

La Figure 2.11 montre les deux niveaux d'interconnexion entre le réseau TISPAN et l'usager. Au niveau service, une authentification au niveau applicatif est effectuée. Au niveau réseau, une authentification réseau est appliquée (explicite ou implicite).

L'usager a accès à plusieurs interfaces avec le réseau TISPAN. Pour les terminaux supportant SIP, ils peuvent utiliser l'interface avec le sous-système IMS. Pour les terminaux POTS standards, une interface avec le sous-système PES est disponible avec une passerelle qui peut résider chez le client ou dans le réseau de l'opérateur. Il existe aussi une interface avec les applications qui permet à l'usager d'avoir accès ou de modifier les informations sur ses services. De plus, il existe une interface entre l'usager et le NASS afin de lui permettre de se connecter au réseau et de recevoir les informations de configuration. Enfin, il existe une interface non-réglementée dans la version 1 des NGN du TISPAN entre l'équipement de l'usager et le RACS.

2.3 MSF

Le *MultiService Forum* (MSF), fondé en 1998, est une association de plusieurs fournisseurs de services et d'équipements. Son but est de développer et promouvoir une architecture ouverte pour les systèmes multi-services commutés. Il prône l'interopérabilité entre les différents fournisseurs pour accélérer le développement des NGN. Ses principales activités sont :

- de développer des ententes d'implémentation inter-fournisseurs ;
- de promouvoir la compatibilité internationale ;
- de collaborer avec les organismes de standardisation.

Le MSF se divise par sujets d'intérêt et chacun de ceux-ci forme un groupe de travail. Voici la liste des principaux groupes de travail :

- l'architecture ;
- l'interopérabilité ;
- les protocoles.

Les prochaines sections découlent des documents suivants :(MSF, 2005a) et (MSF, 2005b).

2.3.1 Architecture globale

La Figure 2.12 présente la deuxième version de l'architecture globale du MSF. Les principaux éléments sont les suivants :

- le *Signalling/Trunking Gateway* ;
- l'*Access Gateway* ;
- le *SIP User Agent* ;
- l'*Edge Router* ;
- le *Session Border Gateway - Network Edge* (SBG-NE) ;
- le *Session Border Gateway - Network Core* (SBG-NC) ;
- le *Session Border Gateway - Customer Edge* (SBG-CE) ;
- le *Call Agent* ;
- le *Bandwidth Manager* ;
- le *Media Server* ;
- le *Service Broker* ;
- l'*Application Server* ;
- le *Service Logic Gateway* ;

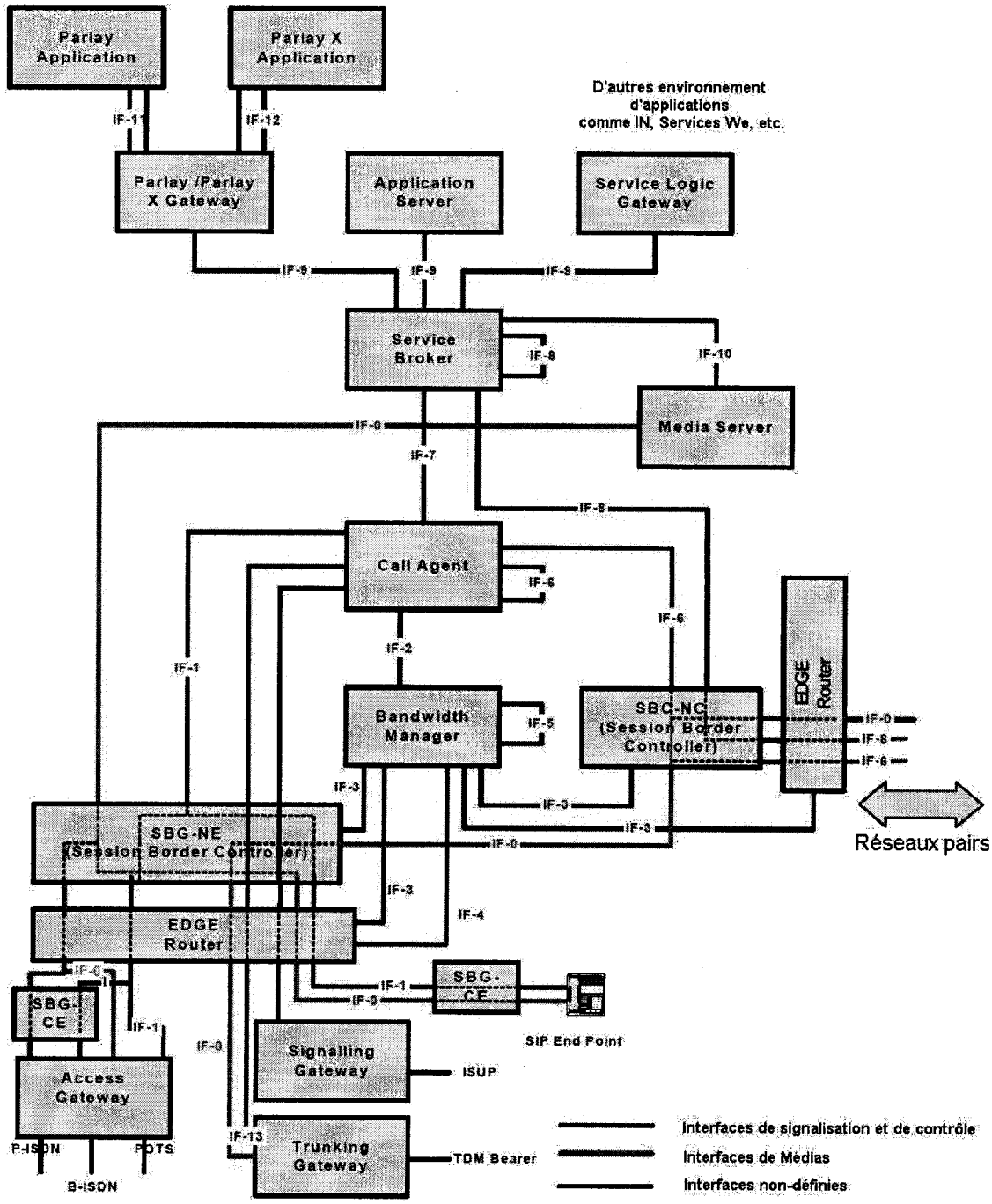

FIGURE 2.12 Architecture globale du MSF version 2

- le *Parlay / Parlay X Gateway* ;
- le *Parlay Application* ;
- le *Parlay X Application.*

Le nœud *Signalling/Trunking Gateway*

Le *Signalling Gateway* et le *Trunking Gateway* permettent l'accès au réseau PSTN basé sur la signalisation SS7 et vice-versa. Le *Signalling Gateway* permet d'effectuer le contrôle entre la signalisation SS7 et le *Call Agent.* Le *Trunking Gateway* permet la conversion entre un appel sur le système PSTN et un sur le système *Voice over IP* (VoIP), sous la direction du *Call Agent* via le protocole MGCP (*Media Gateway Control Protocol*) ou H.248.

Le nœud *Access Gateway*

L'*Access Gateway* permet le support des combinés POTS (*Plain Old Telephone Service*). Il sert de proxy SIP ou MGCP au nom du combiné POTS. Ce nœud peut être présent dans le réseau de l'opérateur ou dans l'équipement de l'usager.

Le nœud *SIP User Agent*

Ce nœud effectue la terminaison de la communication SIP (*Session Initiation Protocol*).

Le nœud *Edge Router*

Ce nœud permet de router le trafic dans le réseau dorsal de l'opérateur. Il effectue aussi le contrôle d'admission du trafic pour respecter les règles de QdS sous le contrôle du BM (*Bandwidth Manager*) et le marquage de flots. Il effectue seulement du traitement au niveau IP et ne touche pas aux protocoles des couches supérieures.

Le nœud SBG-NE

Ce nœud agit comme un point de démarcation (*edge*) du réseau et possède les fonctions suivantes :

- le contrôle de sessions pour effectuer le lien entre la signalisation et les données ;
- l'application et la gestion du NAT pour cacher les adresses internes et la topologie du réseau ;
- la gestion de la sécurité pour prévenir et détecter les intrusions.

Le SBG-NE peut communiquer avec le *Bandwidth Manager* pour effectuer le contrôle d'admission.

Le nœud SBG-NC

Ce nœud a un comportement similaire au SBG-NE, mais il sert pour l'interconnexion entre deux réseaux d'opérateurs.

Le nœud SBG-CE

Ce nœud est aussi similaire au SBG-NE, mais il est déployé sur le site de l'usager.

Le nœud *Call Agent*

Ce nœud permet d'établir les sessions, de les détruire, de les contrôler et de les router. Il génère aussi les données pour la facturation. Il communique avec les applications ou le *Service Broker* pour fournir des services et il effectue des requêtes de bande passante au *Bandwidth Manager*. Chaque terminal d'usager est contrôlé par un *Call Agent*. Il enregistre aussi les *SIP User Agent*. De plus, il se sert des informations de routage pour :

- configurer les appels pour les usagers enregistrés localement ;
- transférer la signalisation au bon *Call Agent* (intra-domaine) ;
- transférer la signalisation au bon domaine (inter-domaines).

Le nœud *Bandwidth Manager*

Ce nœud permet de contrôler la QdS dans le réseau. Plus précisément, il est responsable d'allouer et de détruire les allocations de bande passante et de contrôler l'accès aux ressources pour chaque session en assignant les règles adéquates au *Edge Router*. Il garde aussi des traces pour savoir à tout moment quelles sont les ressources utilisées et par conséquent disponibles. Il s'en sert pour effectuer le contrôle d'admission. Ce nœud peut être distribué dans le réseau de manière à ce que chaque *Bandwidth Manager* contrôle une partie du chemin. L'interface avec le *Edge Node* lui permet de faire un contrôle par flot et l'interface avec le *Core Router* lui permet de contrôler par agrégat.

Le nœud *Media Server*

Ce nœud fournit quelques fonctions multimédias pour les autres nœuds (exemple : pour les serveurs d'applications) comme :

- jouer des messages d'annonce ;
- détecter et générer du *tone* ;
- effectuer la gestion des fax ;
- faire mixage des appels pour les appels conférences ;
- effectuer la reconnaissance de la voix ;
- faire la conversion du texte à la parole et de la parole au texte.

Le nœud *Service Broker*

Ce nœud permet un contrôle de haut niveau des applications et des services d'une session. Il permet à plusieurs applications et services de coopérer sur une seule session. De plus, il communique directement avec les serveurs d'application.

Le nœud *Application Server*

Ce nœud exécute un service ou plusieurs services.

Le nœud *Service Logic Gateway*

Ce nœud agit comme un serveur d'application SIP qui effectue la redirection des requêtes vers le *Service Broker*. Il permet d'exporter une interface standard vers les serveurs d'applications non-SIP.

Le nœud *Parlay / Parlay X Gateway*

Ce nœud est un *Service Logic Gateway* qui exporte l'API (*Application Programming Interface*) Parlay et Parlay X vers les applications. Parlay permet entre autre les fonctions suivantes : le contrôle d'appels, le contrôle de conférences, l'interaction entre les usagers par audio et par texte et le contrôle de la facturation. Parlay X est plus léger et a moins de fonctionnalités que Parlay. Par exemple, il implémente les fonctions suivantes : la localisation d'un usager et la capacité d'établir un appel entre deux usagers.

Le nœud *Parlay Application*

Ce nœud exécute un ou plusieurs services. Il est engagé par le *Parlay Gateway* sous le contrôle du *Service Broker*.

Le nœud *Parlay X Application*

Ce nœud possède les mêmes fonctions que le nœud *Parlay Application*, mais il utilise le protocole Parlay X.

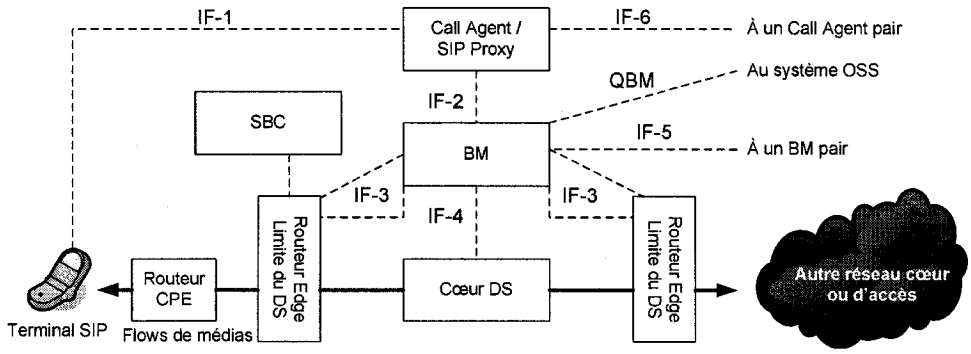

FIGURE 2.13 Architecture de contrôle pour la QdS

2.3.2 Architecture de contrôle des ressources

La Figure 2.13 présente l'architecture de contrôle d'appels et de bande passante du MSF. Le but de cette architecture et de fournir un équivalent à la QdS du PSTN sur un réseau à commutation de paquets.

Les nœuds impliqués dans le système de contrôle de QdS sont :

- le *Call Agent* qui effectue la demande de bande passante ;
- le BM (*Bandwidth Manager*) qui reçoit la demande et qui avec sa vue globale des ressources disponibles effectue le contrôle d'admission, puis la réservation par flot au Routeur Edge (*Edge Router*) et par agrégat au Routeur Coeur (*Core Router*) ;
- le Routeur Edge qui effectue la classification et le marquage du trafic par flot selon les informations reçues du BM ;
- le Routeur Coeur qui permet la configuration d'agrégats (tunnels) sous le contrôle du BM ;
- le SBC (*Session Border Controller*) qui permet de contrôler le NAT pour les services multimédias.

Le *Bandwitdh Manager* (BM) peut être distribué dans le réseau de manière à ce que chaque unité contrôle une partie des ressources. Deux modèles sont énoncés : celui hiérarchique et celui entre pairs. Celui hiérarchique permet d'avoir plusieurs

niveaux de BM. Cela permet une grande flexibilité pour les grands réseaux où plusieurs BM sont installés à la base de celui-ci et la couche suivante comporte moins de BM et une vision plus simpliste (par agrégats) du réseau. Avec celui entre pairs, il est possible de fournir un seul point de contact pour les *Call Agents*. Par la suite, un protocole est utilisé pour trouver automatiquement avec quels BMs communiquer. Il existe aussi des modèles hybrides. Par exemple, le modèle hiérarchique peut être utilisé intra-domaine et le modèle par paires pour communiquer entre les domaines (inter-domaines).

Le MSF a définit son architecture de réservation de ressources (QdS) pour les technologies de transport suivantes : MPLS et IPv6 (Diffserv sans connexion). Il est dit que la solution idéale serait MPLS sur IPv6, mais cela n'est pas encore possible.

2.4 PacketCable

Le projet *PacketCable* est une initiative de CableLabs. Le but principal est de développer des spécifications pour des interfaces interopérables afin de fournir des services multimédias en temps réel. Le projet utilise la technologie du modem câble et celle IP pour le transport. Il existe aussi une certification *PacketCable* qui vise à établir quels produits sont compatibles avec ses normes et à valider son architecture. L'avantage d'être compatible avec les normes *PacketCable* est la possibilité d'offrir un large éventail de services, incluant les services téléphoniques et étendus, à moindre coût. Du côté des usagers, ils pourront avoir accès à plus de services.

Les sections suivantes découlent des documents suivants :(PacketCable, 2005b) et (PacketCable, 2005a).

2.4.1 Architecture globale

La Figure 2.14 montre les composantes de l'architecture fonctionnelle qui sont présentes dans la version 1.5 des spécifications de *PacketCable*.

Les éléments suivants sont présents dans cette architecture :

- le *Multimedia Terminal Adapter* (MTA) ;
- le *Cable Modem* (CM) ;
- l'*Hybrid Fiber Coaxial (HFC) Access Network* ;
- le *Cable Modem Terminaison System* (CMTS) ;

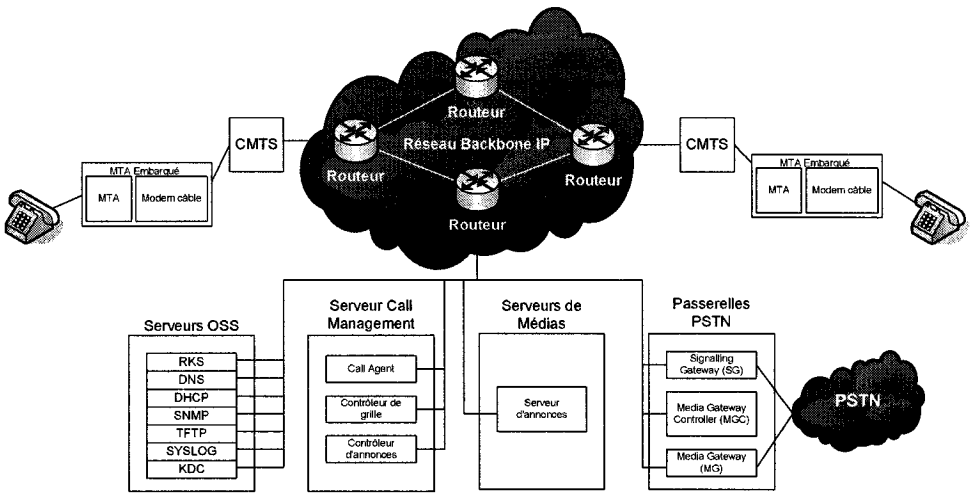

FIGURE 2.14 Architecture fonctionnelle de PacketCable

- le *Call Management Server* (CMS) ;
- le *PSTN Gateway* ;
- l'*OSS (Operational Support Systems) Back Office Components* ;
- l'*Announcement Server* (ANS).

Le nœud MTA

Ce nœud est l'équipement de l'usager. Il a deux interfaces : celle qui fait face au client et celle qui fait face au réseau. Il est connecté au réseau par le réseau d'accès HFC. Ses principales fonctions sont les suivantes :

- effectuer la signalisation d'appels jusqu'au CMS ;
- effectuer la signalisation pour la QdS jusqu'au CMTS ;
- authentifier, assurer la confidentialité et l'intégrité des messages ;
- effectuer le lien entre les flots multimédias et les services de transport ;
- effectuer l'encodage et le décodage des flots multimédias ;
- rendre disponible une interface téléphonique.

Le nœud CM

Ce nœud est un modulateur/démodulateur qui se trouve dans l'équipement de l'usager. Il permet la transmission de données par le câble. Il permet aussi la classification du trafic par flots, le contrôle de débit et le contrôle des files d'attentes prioritaires.

Le réseau *HFC Access Network*

Le réseau d'accès HFC (*Hybrid Fiber Coaxial*) est bidirectionnel et à média partagé. Il a comme fonction primaire le transport des données.

Le nœud CMTS

Ce nœud permet la connectivité pour échanger les données avec le CM. De plus, il supporte des fonctions supplémentaires pour le CM au travers du *HFC Access Network*. Voici les fonctions principales du CMTS :

- contrôler la QdS requise par le CM (entre autres avec sa grille dynamique) ;
- classifier les paquets arrivés du réseau de transport en direction du CM ;
- allouer la bande passante montante et celle descendante ;
- enregistrer les quantités d'informations transmises et reçues par le CM.

Le nœud CMS

Ce nœud permet de contrôler les appels et la signalisation du MTA, CMTS et du *PSTN Gateway*. Il comporte les sous-éléments suivants :

- le *Call Agent* (CMS/CA) qui permet les services de signalisation ;
- le *Gate Controller* (CMS/GC) qui coordonne et contrôle toutes les autorisations de QdS ;
- le *Media Gateway Controller* qui contrôle le *PSTN Gateway*.

Le nœud *PSTN Gateway*

Ce nœud permet au MTA de communiquer avec le PSTN par l'utilisation d'une passerelle (*PSTN Gateway*). Il comporte les sous-éléments suivants :

- le *Media Gateway Controller* (MGC) qui maintient l'état des appels et contrôle le fonctionnement général du *PSTN Gateway* ;
- le *Signalling Gateway* (SG) qui permet l'interconnexion du protocole de signalisation SS7 et le réseau IP ;
- le *Media Gateway* (MG) qui termine le chemin des données entre le PSTN et le réseau IP et effectue la conversion du média.

Les nœud *OSS Back Office Components*

Ce système contient les composantes de gestion de l'entreprise, du réseau et des

services. Il transporte aussi les informations pour la facturation. Ses fonctions principales sont :

- la gestion des erreurs ;
- la gestion de la performance ;
- la gestion de la sécurité ;
- la gestion des acomptes ;
- la gestion de la configuration.

Ses principaux éléments sont :

- le *Key Distribution Center* (KDC) qui effectue l'authentification des MTA ;
- le *Dynamic Host Configuration Protocol Server* (DHCP) qui alloue les adresses IP aux MTA ;
- le *Domain Name System Server* (DNS) qui permet de résoudre l'allocation entre les adresses IP et les noms de domaines ;
- le *Trivial File Transfer Protocol Server or Hypertext Transfer Protocol Server* (TFTP ou HTTP) qui permet la configuration des MTA ;
- le *SYSLOG Server* qui collecte les événements du réseau ;
- le *Record Keeping Server* (RKS) qui permet d'assembler les données pour créer des CDR (*Call Detail Records*) et les transmettre au système de facturation.

Le nœud ANS

Ce nœud gère et génère des tonalités ou des messages en fonction des événements qui se produisent dans le réseau.

2.4.2 Architecture de contrôle des ressources

La Figure 2.15 présente le modèle haut niveau de la séparation entre les sessions et les ressources dans le modèle de *PacketCable*. Le *Resource Control Domain* (RCD) correspond au regroupement des éléments qui fournissent la connectivité et la gestion des règles pour contrôler les ressources du réseau. Il est constitué du CMTS et du *Policy Server* (PS). Le *Service Control Decision* (SCD) est le regroupement des éléments qui fournissent les services et le contenu aux usagers. Il peut avoir un ou plusieurs SCD(s) pour un RCD. L'*Application Manager* réside dans le SCD.

La Figure 2.16 présente l'architecture multimédia de *PacketCable*. Voici le rôles des principaux éléments de cette architecture :

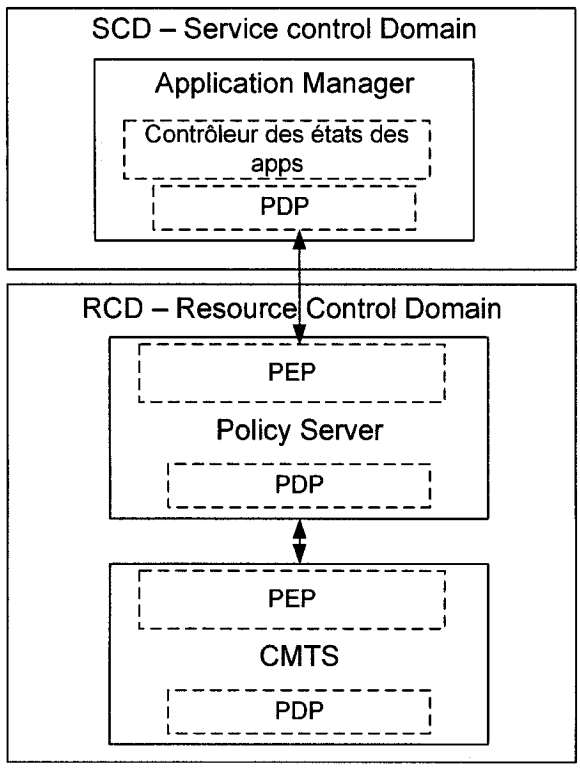

FIGURE 2.15 Domaines de contrôle de sessions et de ressources

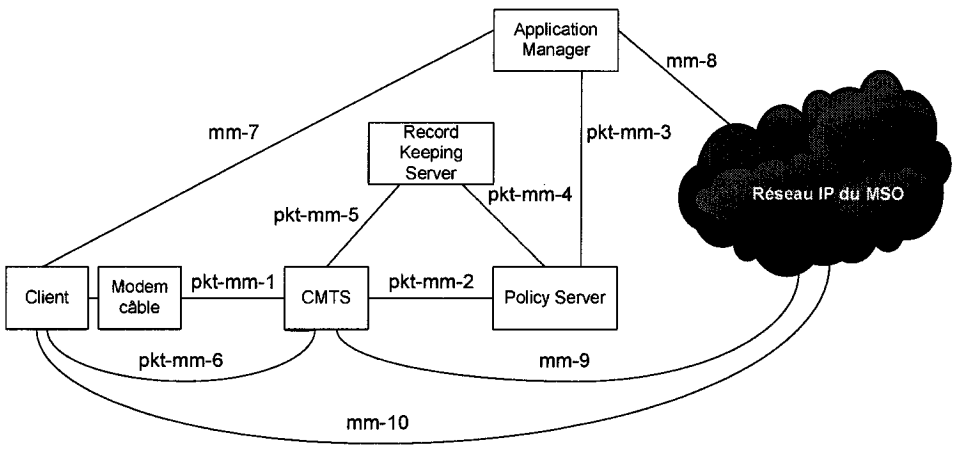

FIGURE 2.16 Architecture multimédia de PacketCable

- l'*Application Manager* est responsable de gérer et contrôler l'état des applications et des sessions et d'appliquer les règles pour la QdS dans le SCD ;
- le *Policy Server* est responsable de gérer les relations entre les *Applications Managers* et les CMTS et d'appliquer les règles de QdS dans le RCD ;
- le CMTS est responsable d'effectuer le contrôle d'admission et de contrôler les ressources du réseau.

Les prochaines sections décrivent le rôle des différentes interfaces de l'architecture multimédia de *PacketCable.*

Interface CMTS-CM

Le CM peut effectuer une requête de QdS au CMTS. Le CMTS peut aussi demander au CM de modifier un de ses paramètres de QdS par cette interface.

Interface PS-CMTS

Cette interface permet de pousser les règles à partir du PS sur le CMTS ou de demander les règles au PS à partir du CMTS. Elle permet aussi d'effectuer une requête de QdS en mode proxy à la demande du client.

Interface AM-PS

Le AM peut demander au PS d'installer les règles d'une décision au CMTS à la demande du client.

Interface PS-PKS

Le PS peut envoyer des messages au RKS pour garder des traces des règles de réservations.

Interface CMTS-RKS

Le CMTS envoi des messages au RKS pour garder des traces des requêtes de QdS et de l'utilisation des flots.

Interface Client-CMTS

Le client peut utiliser cette interface pour directement effectuer une requête de QdS.

Interface Client-AM

Le client peut se servir de cette interface pour demander au AM d'effectuer ou contrôler des requêtes de ressources (QdS).

Interface AM-Peer

L'AM peut se servir de cette interface pour interagir avec d'autres nœuds qui sont aussi impliqués dans l'application.

Interface CMTS-MSO-Managed IP Network

Cette interface peut être utilisée pour le contrôle de la QdS bout-en-bout (pas seulement dans le réseau d'accès).

Interface Client Peer

Le client peut se servir de cette interface pour communiquer avec d'autres entités impliqués dans l'application.

CHAPITRE 3

INTERFACE DE GESTION DES SERVICES

Le monde des télécommunications est présentement en grand changement. En effet, de plus en plus d'utilisateurs migrent des réseaux fixes aux réseaux mobiles. Cependant, pour l'instant, la qualité de service ainsi que la disponibilité des services sont encore de beaucoup supérieures dans les réseaux fixes. Pour contrer ces problèmes et pour effectuer la convergence entre le monde câblé, le monde sans fil et les services des usagers, plusieurs organismes s'impliquent dans la standardisation des réseaux de prochaine génération. Ces réseaux permettront une uniformité au niveau des services et de leur contrôle, peu importe le type d'accès utilisé. Un des organismes les plus actifs et qui se démarque le plus des autres se nomme TISPAN. Son architecture a été expliquée au chapitre précédent. Bien que son évolution soit très rapide, plusieurs aspects n'ont pas encore été abordés, dont la mobilité et le contrôle des services. La solution proposée dans ce chapitre servira donc de commencement pour la gestion de la mobilité et le contrôle des services dans l'architecture du TISPAN. Nous proposons un protocole basé sur l'architecture des NGN du TISPAN permettant de contrôler les ressources, les services et la facturation d'un usager lorsque celui-ci utilise un réseau d'accès appartenant à son fournisseur d'attache ou à un autre fournisseur.

Organisation de la proposition

La proposition de la solution est segmentée en trois parties :

1. la mise en contexte qui a comme objectif de situer la solution par rapport aux réseaux actuels et ceux de prochaine génération ;
2. la présentation des différentes architectures de haut niveau proposées qui seront utilisées pour l'élaboration de la solution ;
3. l'explication de la solution en trois volets.

3.1 Mise en contexte de la solution

Le problème que nous abordons touche plusieurs parties du réseau : l'accès, le contrôle et les services. De plus, ces différentes parties peuvent être distribuées à plusieurs localisations physiques ou virtuelles. En effet, le réseau d'accès et de contrôle peuvent appartenir à une compagnie et le contrôle des services à une autre. Cette situation amène de nouvelles possibilités d'affaire comme les opérateurs de réseaux mobiles virtuels (MVNO - *Mobile Virtual Network Operator*). Les MVNO permettent aux opérateurs de gérer seulement la partie des services et d'utiliser le réseau de contrôle et d'accès d'un autre opérateur. Le modèle classique dans lequel l'opérateur est propriétaire du réseau de contrôle et d'accès ainsi que de la partie de contrôle des services est encore possible. La Figure 3.1 montre la séparation des domaines qui permet ces nouvelles possibilités d'affaire. Dans ce projet, nous supposons que le réseau visité sert de réseau d'accès et de contrôle et que le réseau d'attache fournit les services. Cependant, il est possible d'utiliser des services fournis par le réseau visité. Cela peut être particulièrement utile pour les services de localisation qui doivent utiliser la position courante dans le réseau visité pour pouvoir fonctionner adéquatement. En effet, si l'usager est abonné à Montréal et qu'il est présentement en déplacement en France, cela serait inopportun de rechercher un restaurent ou un taxi à Montréal lorsqu'il en a besoin en France. Bien que la séparation des domaines soit correctement définie, il n'en est pas de même des mécanismes de communication inter-domaine et de l'architecture nécessaire pour supporter ces mêmes mécanismes. Dans ce chapitre, nous proposons une architecture ainsi qu'un protocole pour permettre à l'opérateur d'attache de contrôler les ressources, les services et la facturation d'un usager qui n'utilise pas son réseau d'accès. Le protocole pourra aussi être utilisé à l'intérieur même du domaine d'un opérateur possédant les trois parties du réseau.

Dans la prochaine section, chacune des parties de la Figure 3.1 sera décrite avec de plus amples détails.

3.2 Architecture de la solution

Puisque l'architecture interne de chacune des parties du réseau : accès, contrôle et services n'est pas clairement définie, nous proposons d'abord notre vision de celle-ci.

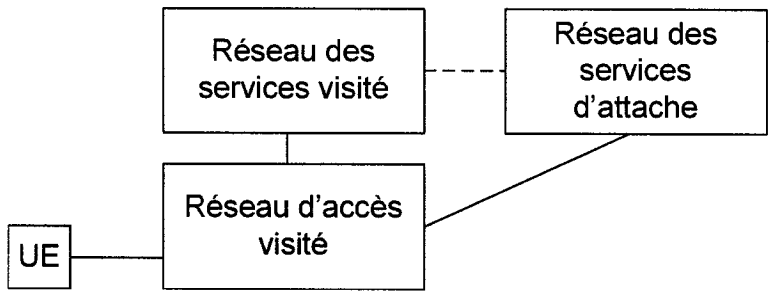

FIGURE 3.1 Séparation des différents domaines

La Figure 3.2 montre l'architecture du réseau d'accès visité. Cette partie du réseau est utilisée par un usager pour se connecter physiquement au réseau lorsqu'il est en déplacement ou lorsqu'il est dans son réseau d'attache. Cette partie du réseau a les fonctions principales suivantes :

- la connectivité physique (L2) et IP de l'usager (implique principalement le NASS) ;
- la gestion et le contrôle d'admission des ressources de toutes les sections du réseau (implique principalement le RACS) ;
- l'interconnexion IP du réseau avec d'autres parties du réseau, avec les réseaux d'attache ou avec d'autres réseaux.

Entre l'usager et le noeud *Techno*, on retrouve le réseau d'accès qui est dépendant de la technologie. Entre l'AN (*Access Node*) et l'AES (*Access Edge Site*), on retrouve le réseau d'accès indépendant de la technologie. Présentement, la technologie qui a le plus de chance de s'y retrouver c'est Ethernet optique avec un protocole du type DiffServ (Blake *et al.*, 1998) (Koucheryavy *et al.*, 2006) pour le contrôle de la QdS. Entre l'AES et le BES (*Border Edge Site*) on retrouve le réseau d'agrégation. Ce réseau contient un ou plusieurs serveurs P-CSCF (*Proxy-Call Session Control Function*) qui permettent de diriger la signalisation pour la gestion des services dans le bon réseau d'attache. Dans ce réseau, un protocole du type HPMRSVP-TE (Ouellette, 2006) ou NSIS (NSIS, 2005) pourra être utilisé. Le noeud AES et le noeud BES servent à contrôler les ressources ainsi qu'à contrôler les services. Il existe aussi un lien entre le réseau d'accès et un LEA (*Legal Enforcement Agency*) pour permettre de transmettre des informations aux autorités légales à la demande. Un autre BES réside sur la frontière de démarcation entre le réseau coeur et le réseau dorsal qui permet l'interconnexion entre les domaines. Un SG (*Security Gateway*)

permet de sécuriser ces interconnexions. Les éléments suivants, qui sont en rouge sur la Figure 3.2, seront touchés dans ce projet :

- le NASS ;
- le RACS ;
- l'AES ;
- le BES ;
- l'interface entre le NASS et le RACS ;
- l'interface entre le RACS et l'AES ;
- l'interface entre le RACS et le BES.

Les interfaces suivantes, qui sont en pointillé sur la Figure 3.2, devront être définies dans des projets subséquents :

- l'interface du RACS pour contrôler les ressources dans le réseau d'accès ;
- l'interface du RACS pour contrôler les ressources entre les opérateurs (sur la dorsale).

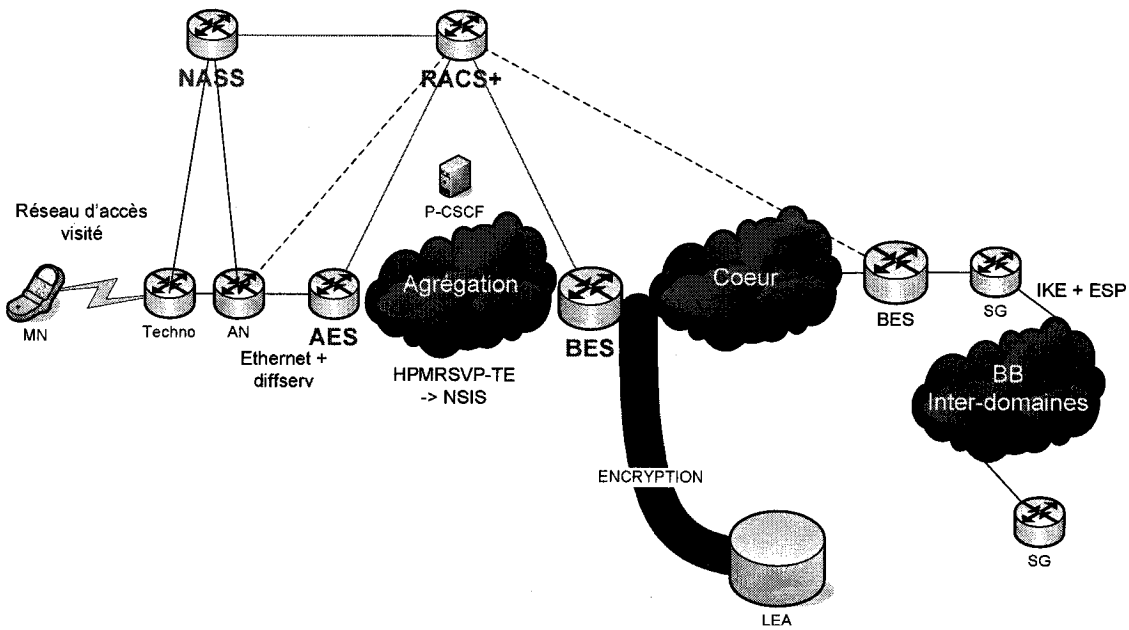

FIGURE 3.2 Architecture du réseau d'accès visité

La Figure 3.3 montre que le RACS peut être divisé en plusieurs éléments qui sont chacun responsable de la gestion des ressources dans des parties distinctes du réseau. On pourrait par exemple retrouver les nœuds RACS suivants :

- le RACS-A pour le contrôle du réseau d'accès (il pourra être dépendant ou non de la technologie d'accès) ;
- le RACS-AGG pour le réseau d'agrégation ;
- le RACS-C pour le réseau coeur ;
- le RACS-BB pour la dorsale ;
- le RACS central pour un point de contact unique.

La communication entre les différents RACS peut s'effectuer de façon pair à pair (interfaces en pointillé), de façon hiérarchique (tout passe par le nœud au sommet) ou de façon hybride. L'article (Bouras et Stamos, 2005) a étudié quelques uns de ces scénarios. Les interfaces inter-RACS du même domaine et la séparation des différents nœuds devront être traitées plus précisément dans un prochain projet de recherche. L'article (Krishnamurthy *et al.*, 2005) aborde la communication distribuée entre les RACS (*Bandwidth Broker* de différentes domaines.

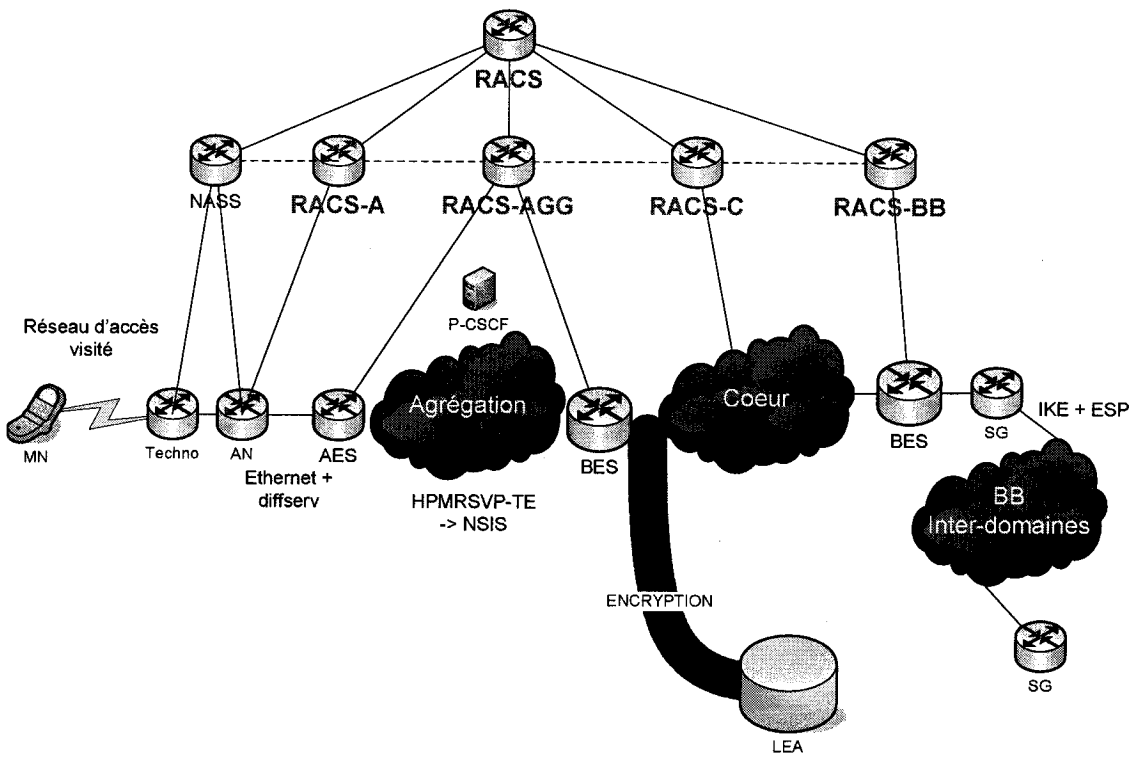

FIGURE 3.3 Architecture du réseau d'accès visité avec la division du RACS

La Figure 3.4 montre l'architecture du réseau d'attache qui s'occupe des services. La même architecture peut être utilisée lorsque l'usager est dans son réseau d'accès

d'attache ou dans un visité. L'architecture permet la séparation de l'accès et des services pour des modèles d'affaire de type MVNO et peut aussi être utilisée par les opérateurs qui possèdent tous les niveaux de réseau. Dans la Figure 3.4, il existe deux grands types d'applications : celles de l'IMS et celles qui utilisent d'autres systèmes. Chacun des deux types peut s'interconnecter avec un tier fournisseur de services par un SG (*Security Gateway*) pour fournir une plus vaste gamme de services. Le réseau d'attache qui s'occupe des services s'interconnecte avec un réseau d'accès par le SG. Le principe du I-X (*Interrogating*), P-X (*Proxy*) et S-X/H-X (*Serving/Home*) est utilisé. Le P-X sert de *proxy* pour envoyer un message au I-X qui sert de point de contact unique dans un domaine et redirige le message au bon S-X. Ce principe est utilisé pour contacter le NASS, le RACS et l'IMS. Le UAAF sert de point de contact pour avoir accès au profil de l'usager qui peut résider par exemple sur un serveur AAA (*Authentication Authorization Accounting*). Le CLF sert de point de contact aux applications pour localiser l'usager et pour avoir accès à leur profil. Il sert aussi de lien avec le HA (*Home Agent*) pour assurer la mobilité IP. On suppose aussi que le S-CSCF (H-CSCF) permet d'accéder aux applications IMS et non-IMS. Pour réserver des ressources, l'IMS communique avec le SPDF qui s'assure du respect des règles locales et transmet la requête au H-RACS qui sert de proxy pour transmettre la requête au S-RACS qui se trouve dans le domaine visité.

La Figure 3.5 montre l'architecture de gestion des services du réseau visité. Cette architecture permet à l'usager en déplacement l'accessibilité à d'autres services . De plus, pour tout ce qui touche aux services de localisation, l'usager en visite doit utiliser cette architecture. Elle correspond à une version simplifiée de l'architecture du réseau d'attache qui s'occupe des services. En effet, elle ne garde aucune information sur l'usager. Par contre, il pourrait être intéressant de garder un profil de visite dans le réseau visité pour permettre certains traitements sur les services de l'usager. Par exemple, lorsqu'un ordre de la cour affectant un usager existe dans le pays visité, il serait intéressant de sauvegarder à l'aide d'un profil local au réseau visité qu'il faut enregistrer ses communications. Si l'on décide de garder des informations sur l'usager, l'architecture de gestion des services du réseau visité devient la même que celle du réseau d'attache sans le HA (*Home Agent*).

La Figure 3.6 suivante est tirée du WG7 (Sécurité) du TISPAN. La séparation des domaines est semblable avec ce qui est proposé dans ce projet à quelques détails près. Il semble cependant manquer quelques interfaces et quelques-unes semblent

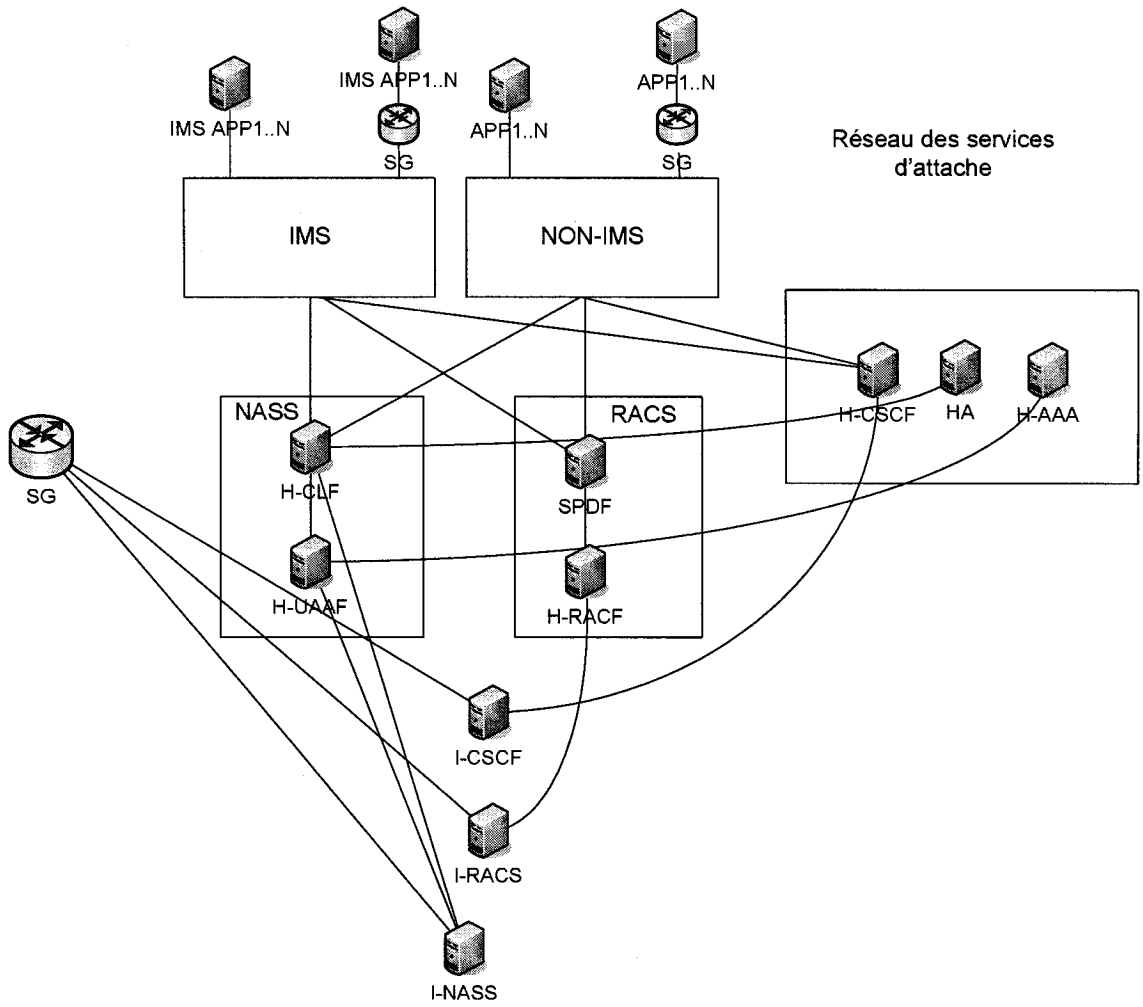

FIGURE 3.4 Architecture du réseau d'attache pour les services

superflues pour assurer le bon fonctionnement de cette architecture. De plus, il manque certains détails, mais la vision de haut niveau que la figure présente est intéressante. Le nœud important dans cette figure est le SEGF (*SEcurity Gateway Function*) qui sert de passerelle de sécurité. Il serait intéressant de regrouper les rôles fonctionnels de ces différents nœuds dans un SEGF global (qu'on pourrait nommer SG pour *Security Gateway*) pour avoir un point unique de contact. La séparation entre les domaines n'est pas identique à notre vision. La plus grande différence est la segmentation du réseau de transport entre l'accès et le reste (agrégation et coeur). Dans notre vision, nous supposons que le transport n'est pas segmenté et qu'il fait entièrement partie du réseau visité. Pour le moment, nous ne trouvons pas cette

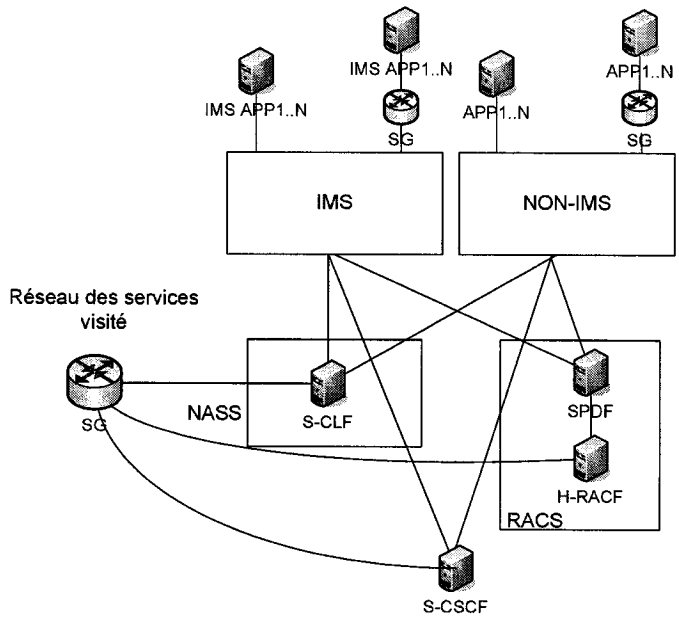

FIGURE 3.5 Architecture du réseau visité pour les services

séparation nécessaire pour solutionner notre problème. De plus, ses répercutions sur notre solution seraient minimes et c'est pourquoi nous en ferrons abstraction.

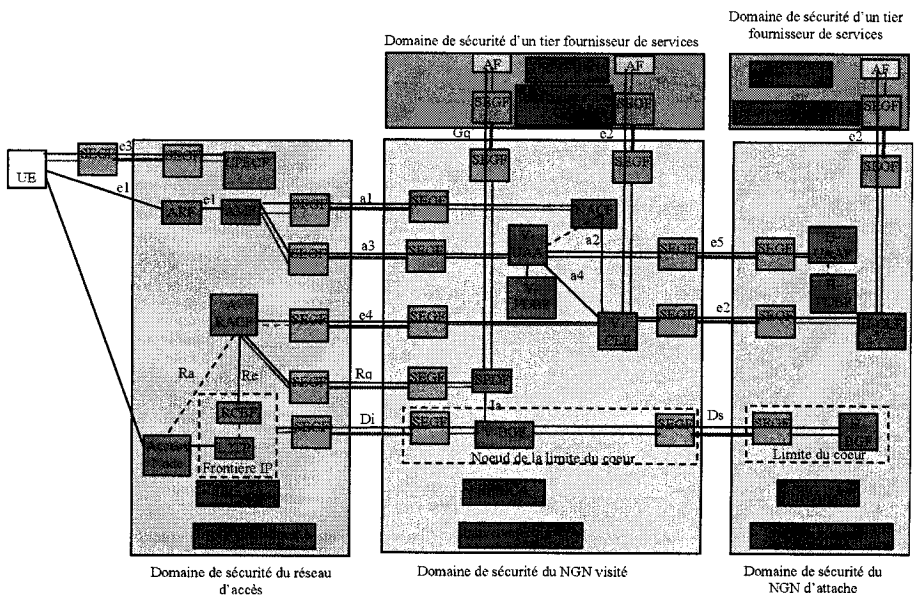

FIGURE 3.6 Architecture proposée par le WG7 du TISPAN

Cependant, cette séparation pourrait être considérée dans un projet futur. Elle pourrait être utile pour effectuer une division du réseau de transport (un ou plusieurs opérateurs pour l'accès et un opérateur différent pour le réseau IP). Cela pourrait probablement engendrer de nouveaux modèles d'affaire.

3.3 Explication de la solution

La solution se divise en trois volets :

1. la modification du profil réseau, sa segmentation et les messages de synchronisation ;
2. la gestion des ressources virtuelles du H-RACS et les messages de synchronisation entre le H-RACS et le V-RACS ;
3. l'échange d'informations pour facturer adéquatement le client.

3.3.1 Volet 1

Dans ce volet, le profil réseau sera segmenté en deux parties et on y ajoutera plus d'informations pour la QdS et pour le contrôle des services. De plus, on créera les message de synchronisation et d'échange des différents profils. Actuellement le TISPAN a défini deux sortes de profils :

1. le profil réseau qui contient de l'information sur l'accès au réseau de l'usager et optionnellement sur la QdS et sur l'état des grilles ;
2. le profil service qui contient de l'information sur les abonnements aux différents services de l'usager.

Voici les tâches effectuées dans ce volet :

- segmentation du profil réseau en deux parties : accès et QdS et contrôle des services ;
- ajout d'informations de QdS par type de flot dans le profil de QdS et de contrôle des services ;
- ajout d'informations de contrôle des services dans le profil de QdS et de contrôle des services ;
- création des messages de transmission et de synchronisation des profils d'accès et de QdS et de contrôle des services entre le réseau visité et le réseau d'attache ;

- création des messages de synchronisation pour le contrôle des services (en fonction des types de contrôles supportés par le réseau visité).

Segmentation du profil réseau

Nous proposons donc dans ce volet de segmenter le profil réseau en deux parties :

1. le profil d'accès qui contient de l'information sur l'accès au réseau de l'usager (utile au NASS) ;
2. le profil de QdS et de contrôle de services qui contient de l'information sur la QdS, sur l'état des grilles et sur le contrôle des services (utile au RACS).

Puisque chacun des profils est utile en premier lieu à des sous-systèmes différents, il semble intéressant de le diviser. De plus, la partie de QdS et de contrôle des services devra faire partie d'un processus de synchronisation entre le réseau d'attache et le réseau visité et ce n'est pas le cas du profil d'accès. Il y a donc au moins deux bonnes raisons de le diviser.

Le profil d'accès ressemblerait à celui présenté au Tableau 3.1. Le profil en entier correspond à une sous-partie du profil réseau présenté dans le document du NASS : (TISPAN, 2005c). Nous y avons seulement ajouté une clé ou un identifiant privé pour authentifier l'usager. De plus, il nous semble judicieux que l'adresse IP globale soit utilisée pour sauvegarder l'adresse IP du HA (*Home Agent*) et que le domaine d'adressage sauvegarde l'adresse du réseau d'attache (sous forme d'un domaine ou d'une adresse publique). Le domaine d'adressage sert donc à trouver le bon opérateur et l'adresse IP à trouver le bon sous-réseau dans le réseau de l'opérateur.

TABLEAU 3.1 Profil d'accès

Éléments d'information	**Description**
ID de l'abonné	L'identité de l'abonné qui demande une connectivité IP
Indicateur privé	Indique si les informations de localisation peuvent être exportées à la couche des services et des applications
Clé ou identifiant de l'usager	Information pour authentifier l'usager
Adresse globale unique	
- L'adresse IP assignée (Home Address)	L'adresse IP de l'équipement de l'usager
- Domaine d'adressage (Domaine pour les I-X (I-RACS, I-NASS, I-CSCF, etc.)	Le domaine d'adressage dans lequel l'adresse est valide et significative

La question que nous nous sommes posés est la suivante : doit-on inclure dans le profil d'accès les adresses de tous les I-X ou non ? Nous croyons que non, car il est plus flexible d'utiliser le domaine avec la technique du I-X (*Interrogating*), du S-X (*Serving*) et du P-X (*Proxy*). Premièrement, il n'est pas nécessaire de modifier le profil à chaque fois qu'un nouveau noeud utilisant cette technique est créé. Deuxièmement, le profil s'en voit simplifié et allégé.

L'autre partie qui résulte de la segmentation du profil réseau est le profil de QdS et de contrôle des services. Cette ancienne partie du profil réseau est présentée dans le Tableau 3.2.

TABLEAU 3.2 Profil réseau sans modification

Profil de QdS	
- Classe de service de transport	La classe de service de transport souscrite par l'usager.
- Bande passante souscrite en amont	La quantité maximale de bande passante souscrite par l'usager en amont.
- Bande passante souscrite en aval	La quantité maximale de bande passante souscrite par l'usager en aval.
- Priorité maximale	La priorité maximale allouée pour une requête de réservation.
- Les Ids des classes d'applications	Identifie les classes d'applications allouées pour utiliser le profil de QdS.
Configuration initiale des grilles	
- Liste des destinations permises	La liste des adresses de destination par défaut, des ports, des préfixes et des intervalles de ports auquels du trafic peut être envoyé.
- Bande passante par défaut en amont	La quantité maximale de bande passante qui peut être utilisée sans autorisation explicite en amont.
- Bande passante par défaut en aval	La quantité maximale de bande passante qui peut être utilisée sans autorisation explicite en aval.

Ajout d'informations de QdS par type de flot

Dans cette sous-section, nous ajoutons au profil présenté au Tableau 3.2 des informations de QdS par type de flot. Ceci est utilisé pour permettre à un usager qui se déplace dans un réseau visité d'apporter avec lui ses configurations de QdS (un mécanisme de synchronisation est présenté dans une prochaine section). De plus, une division par type de flot permet beaucoup plus de flexibilité qu'une configuration par bande passante uniquement. Le profil de QdS et de contrôle des

services avec modifications pour la QdS est présenté dans le Tableau 3.3. Le champ *Classe de service de transport* peut être gardé même si l'on fait une distinction par flot. Par exemple, on pourrait avoir plusieurs classes de vidéo (plusieurs priorités de réservation) et avoir au sein même d'une priorité de vidéo plusieurs types d'utilisateurs (premium, normal, etc.). De cette façon, on pourrait avantager les usagers premiums si la ressource devient saturée ou bien en utilisant des queues prioritaires au sein même d'une priorité de flot. Ce champ n'a pas pour l'instant une utilité très importante, mais nous proposons de le garder quand même. La bande passante totale souscrite dans les deux sens (en amont et en aval) est aussi conservée. Par contre, la *Priorité maximale* et les *identificateurs des classes d'applications* seront inclus pour chaque type de flot. La liste des flots supportés ainsi que des informations sur chacun des flots seront ajoutées.

TABLEAU 3.3 profil réseau avec modifications pour la QdS

Profil de QdS	
- Classe de service de transport (Utilisateur premium ?)	La classe de service de transport souscrite par l'usager.
- Bande passante souscrite en amont (TOTAL)	La quantité maximale de bande passante souscrite par l'usager en amont.
- Bande passante souscrite en aval (TOTAL)	La quantité maximale de bande passante souscrite par l'usager en aval.
- Priorité maximale (??? Par flot)	La priorité maximale allouée pour une requête de réservation.
- Les Ids des classes d'applications (??? Par flot)	Identifie les classes d'applications allouées pour utiliser le profil de QdS.
- Types de flots supportés	Vidéo, audio, data, etc.
- Flot Vidéo	Bande passante souscrite en amont
	Bande passante souscrite en aval
	Priorité maximale pour la réservation
	Classe de service de transport (premium, normal, etc.)
	Les Ids des classes d'applications
...	...
Configuration initiale des grilles	
- Liste des destinations permises	La liste des adresses de destination par défaut, des ports, des préfixes et des intervalles de ports auquels du trafic peut être envoyé.
- Bande passante par défaut en amont	La quantité maximale de bande passante qui peut être utilisée sans autorisation explicite en amont.
- Bande passante par défaut en aval	La quantité maximale de bande passante qui peut être utilisée sans autorisation explicite en aval.

Ajout d'informations de contrôle des services

Le profil QdS et contrôle des services avec les modifications pour le contrôle des services est présenté au Tableau 3.4. Cette section du profil est optionnelle. Une sous-section est attribuée à chaque mécanisme de contrôle des applications. En effet, chacun des mécanismes est identifié par :

- un identificateur, qui devra être standardisé pour être valide inter-domaines ;
- un champ pour le nombre d'arguments qui ne sera pas nécessairement utile si une implémentation du type SOAP (XML) est effectuée, mais il pourra servir pour identifier la version de la fonction de contrôle ;
- une liste variable d'argument(s) qui devront aussi être standardisés entre les domaines.

TABLEAU 3.4 Profil réseau avec modifications pour le contrôle des services

Profil de QdS	
- Classe de service de transport	La classe de service de transport souscrite par l'usager.
- Bande passante souscrite en amont	La quantité maximale de bande passante souscrite par l'usager en amont.
- Bande passante souscrite en aval	La quantité maximale de bande passante souscrite par l'usager en aval.
- Types de flots supportés	Vidéo, audio, data, etc.
- Différents types de flot	Bande passante souscrite en amont
	Bande passante souscrite en aval
	Priorité maximale pour la réservation
	Classe de service de transport (premium, normal, etc.)
	Les Ids des classes d'applications
Configuration initiale des grilles	
- Liste des destinations permises	La liste des adresses de destination par défaut, des ports, des préfixes et des intervalles de ports auquels du trafic peut être envoyé.
- Bande passante par défaut en amont	La quantité maximale de bande passante qui peut être utilisée sans autorisation explicite en amont.
- Bande passante par défaut en aval	La quantité maximale de bande passante qui peut être utilisée sans autorisation explicite en aval.
Configuration initiale du contrôle des services (Optionel)	
ID type de contrôle	Nombre d'argument(s)
Argument 1	Argument 2
...	
...	...

Dans les prochains paragraphes, trois exemples de la partie de contrôle des services du profil de QdS et de contrôle des services sont présentés.

Le Tableau 3.5 montre un exemple de blocage sans avertissement du service de navigation web. Il est important de noter que les valeurs des identificateurs sont données à titre indicatif seulement. Dans les travaux futurs, les identificateurs devront être standardisés.

TABLEAU 3.5 Exemple 1 d'une option du profil de contrôle des services

Contrôle = Blocage sans avertissement (ID=1)	Grandeur = 1 argument
Argument 1 = Service = Navigation web (ID=1)	

Le Tableau 3.6 montre un exemple de blocage avec avertissement du service de navigation web.

TABLEAU 3.6 Exemple 2 d'une option du profil de contrôle des services

Contrôle = Blocage avec avertissement (ID=2)	Grandeur = 2 arguments
Argument 1 = Service = Navigation web (ID=1)	Argument 2 = Message = Blah Blah Blah

Le Tableau 3.7 montre un exemple de blocage sans avertissement du service de navigation web avec la redirection vers un lien web d'information.

TABLEAU 3.7 Exemple 3 d'une option du profil de contrôle des services

Contrôle = Blocage avec avertissement (ID=2)	Grandeur = 2 arguments
Argument 1 = Service = Navigation web (ID=1)	Argument 2 = URL = http ://www.blocage.roger.ca

Voici quelques autres exemples d'options qui pourraient être utilisées dans la partie du profil de contrôle des services :

- blocage avec ou sans avertissement de l'un des services ;

- blocage de contenu ;
- analyse de contenu ;
- ajout d'un message ;
- duplication d'un flot pour analyse ou enregistrement ;
- redirection d'un flot ;
- blocage d'un flot ;
- facturation basée sur le contenu ;
- facturation basée sur le type de flot ;
- blocage ou copie d'un flot encrypté bout à bout ;
- blocage de l'utilisation des routes optimales (MIPv6 (Johnson *et al.*, 2004), HMIPv6 (Soliman *et al.*, 2005)) ;
- introduction de jitters/délais.

Messages de transmission et de synchronisation des profils d'accès et de QdS et contrôle des services

La Figure 3.7 montre l'architecture présentement définie par le TISPAN pour l'échange du profil réseau entre un réseau d'attache et un réseau visité. Le profil réseau s'échange par l'interface *e5* du NASS et il est par la suite passé au RACS par l'interface *e4*). L'interface *e2* sert aux applications pour rechercher l'utilisateur.

Puisque le profil réseau se divise maintenant en deux parties : accès et QdS et contrôle des services, il faut changer le processus d'échange du profil. Le profil d'accès s'échangera inter-NASS comme précédemment et le profil QdS et contrôle de services s'échangera par l'interface inter-RACS (que nous allons créer dans le deuxième volet de la solution) et se synchronisera au niveau des ressources (bande passante, priorité, etc.) et du contrôle des services entre les domaines. Par la suite, le RACS enverra une copie du profil au NASS qui aura déjà authentifié l'usager. Ensuite, le profil complet sera poussé vers le V-CLF qui lui enverra un message au H-CLF. La mobilité des services s'effectuera encore par l'IMS au travers des différents noeuds CSCF.

Messages de synchronisation pour le contrôle des services

On doit créer un protocole de synchronisation pour le contrôle des services. Par exemple, ce protocole peut être utile si le réseau visité ne peut pas supporter

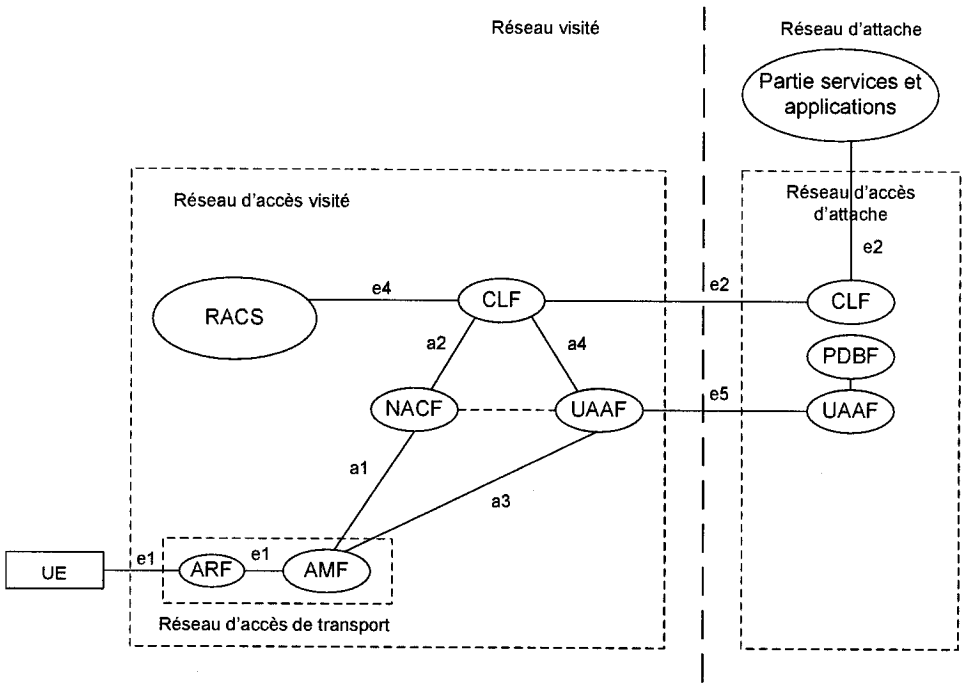

FIGURE 3.7 Architecture actuelle pour l'échange du profil réseau

les options ou les versions des options que l'opérateur d'attache souhaite, il peut forcer la redirection du flot au réseau d'attache. La version peut être reconnue par l'identification explicite de la version dans le profil ou par la reconnaissance des types ou du nombre d'arguments.

Il est important de noter que le nombre d'options de contrôle est théoriquement illimité. Selon la tendance actuelle des marchés, il est de plus en plus possible que l'échange des profils se fera à l'aide du protocole SOAP (XML). Bien que présentement le TISPAN utilise le protocole DIAMETER, SOAP semble plus approprié pour la synchronisation et la gestion des profils. De plus, il est de plus en plus utilisé dans l'industrie.

Les messages de synchronisation pour le contrôle des services (en fonction des types de contrôles supportés par le réseau visité) devraient être inclus à même la synchronisation du profil de QdS et de contrôle des services présenté à la section précédente.

Mise en commun des messages de synchronisation du profil de QdS et de contrôle des services

Il est important de noter que les informations du profil réseau de base ont déjà été définies par le TISPAN. Cependant, aucun type de message sur *e5* n'a été défini. De plus, nous proposons des modifications au profil ainsi que sa segmentation.

Dans les deux prochains paragraphes, nous présentons une liste des différents messages de synchronisation (de transmission) du profil QdS et de contrôle des services qui devront exister entre le réseau visité et le réseau d'attache.

Dans le réseau d'attache :

- RACS d'attache : *Profile-push-visited*, *Profile-pull-visited*, *Profile-sync-visited*, *Profile-resync-visited* ;
- NASS d'attache : *Profile-update* ;
- IMS d'attache : aucun.

Dans le réseau visité :

- RACS visité : *Profile-pull*, *Profile-push*, *Profile-sync*, *Profile-resyns* ;
- NASS visité : *Profile-update* ;
- IMS visité : aucun.

L'action *Push* permet l'envoi du profil et le *Pull* permet de le demander. Pour la synchronisation de la QdS, la plus petite mesure doit être conservée (ex : visité=1Mbps, attache=2Mbps donne un synchronisation à 1Mbps). En plus la synchronisation de la QdS, il doit aussi y en avoir une pour le contrôle des services. Celle-ci s'effectue par refus/acceptation et génération de nouvelles combinaisons d'options de contrôle pour satisfaire les deux parties. Une fois la synchronisation terminée, le RACS doit avertir le NASS (CLF) en lui transmettant le profil qui résulte de la synchronisation (négociation). L'action de re-synchronisation est utile lorsque les profils des usagers ou les configurations du réseau d'attache ou du réseau visité sont changés. Cela permet de considérer dynamiquement la modification du profil de l'usager. Le NASS peut transmettre une notification lorsque le profil de l'usager est modifié et une re-synchronisation peut ensuite en découler. Le RACS peut aussi en être la cause si les politiques du domaine sont changées.

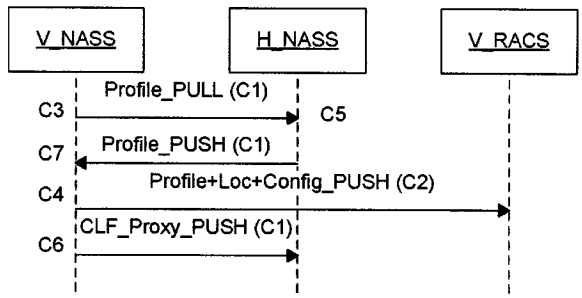

FIGURE 3.8 Diagramme de séquence de téléchargement du profil

La Figure 3.8 montre le diagramme de séquence pour l'envoi du profil avant les modifications proposées. Voici les différentes étapes :

1. le V-NASS a détecté la connexion d'un usager qui appartient pas à son domaine et demande au H-NASS le profil de celui-ci ;
2. le H-NASS envoie le profil réseau de l'usager au V-NASS qui l'authentifie et lui procure une adresse IP ;
3. le profil est transmis au V-RACS pour qu'il effectue les réservations des ressources ainsi que le contrôle des grilles en fonction du profil de l'usager ;
4. le H-CLF est informé de rediriger ses requêtes au V-CLF.

La Figure 3.9 montre le diagramme de séquence pour la synchronisation du profil après les modifications proposées. Voici les différentes étapes :

Section 1

1. le V-NASS a détecté la connexion d'un usager qui n'appartient pas à son domaine et demande au I-NASS de son domaine de rediriger la requête de demande de profil d'accès au I-NASS du domaine d'attache et il trouvera ensuite le bon H-NASS ;
2. le V-NASS informe le V-RACS du début de la séquence pour qu'il puisse lui aussi commencer en parallèle l'échange et la synchronisation du profil QdS et contrôle de services (Section 2) ;
3. la requête de demande d'accès au profil d'accès est redirigée au bon H-NASS (Dans le H-NASS, une requête est envoyée au H-UAAF qui, lui, a accès au H-PDBF qui contient le profil d'accès de l'usager) ;
4. le profil d'accès est envoyé au I-NASS (point de contact bidirectionnel unique pour des raisons de sécurité) qui lui la transmet au I-NASS du domaine visité ;
5. le profil d'accès est transmis au V-NASS qui authentifie l'usager et lui procure une adresse IP ;
6. le V-NASS transmet un message au V-RACS pour l'informer que la configuration d'accès est effectuée et que la configuration est transmise à l'intérieur du V-NASS au V-CLF ;
7. le V-NASS est par la suite en attente du profil de QdS et de contrôle des services synchronisé qui lui sera transmis par le V-RACS.

Section 2

1. le V-RACS demande au I-RACS de son domaine de rediriger la demande de profil de QdS et de contrôle des services au I-RACS du domaine d'attache qui la transmettra au bon H-RACS ;
2. la demande d'accès au profil de QdS et de contrôle des services est redirigée vers le bon H-RACS (dans le H-RACS, le H-RACF a accès au H-PDBF qui contient le profil de QdS et de contrôle des services de l'usager) ;
3. le profil de QdS et de contrôle des services est envoyé au I-RACS (point de contact bidirectionnel unique pour des raisons de sécurité) qui lui le transmet au I-RACS du domaine visité ;
4. le profil est ensuite transmis au V-RACS qui, lui, effectue la synchronisation de la QdS (la valeur la plus restreinte des deux domaines l'emporte) et la synchronisation des options de contrôle des services ;
5. le V-RACS transmet ensuite sa réponse au I-RACS qui, lui, la transmet au bon H-RACS par l'intermédiaire du I-RACS du domaine d'attache ;
6. le H-RACS vérifie les valeurs pour la QdS et les options de contrôle des services (effectue des changements si nécessaire, mais si tout est conforme, il accepte la configuration) ;
7. le H-RACS transmet ensuite le message au I-RACS qui, lui, la transmet au V-RACS ;
8. le V-RACS analyse la réponse et effectue des changements tant que les deux sections ne sont pas acceptées des deux côtés ;
9. lorsque les deux sections (QdS et contrôle des services) sont acceptées par les deux parties, il y a échange dans les deux directions des messages d'acceptation (à l'interne du RACS, les ressources sont réservées et les règles de contrôle des ressources et des services sont configurées) ;
10. le V-RACS informe ensuite le V-NASS en lui envoyant le profil synchronisé ;
11. le V-NASS (V-CLF) informe par la suite le H-NASS (H-CLF) au travers du I-NASS du domaine de l'usager.

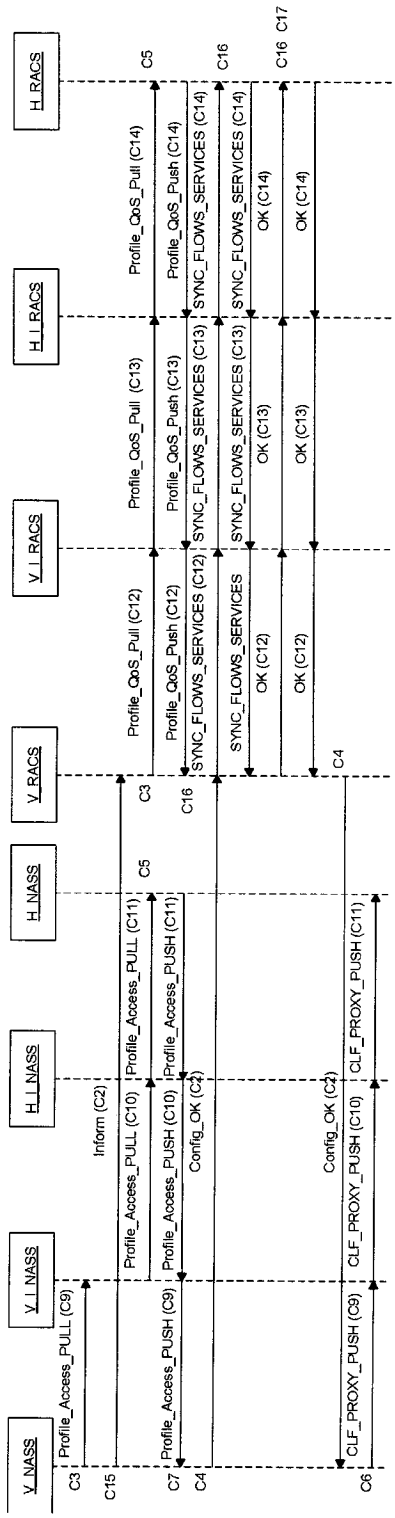

FIGURE 3.9 Diagramme de séquence modifié du téléchargement du profil

3.3.2 Volet 2

Le volet 2 de la solution implique la création d'un mécanisme de contrôle de ressources virtuelles par le H-RACS. En effet, le H-RACS pourra avoir un aperçu en tout temps des ressources utilisées par l'usager dans le réseau visité. De plus, il pourra rediriger les requêtes de demande de ressources en agissant comme un *proxy* vers le réseau visité, car les ressources se trouvent physiquement dans ce réseau et non dans le réseau d'attache.

Voici les tâches effectuées dans ce volet :

- création d'une interface inter-RACS (S-RACF, I-RACF et P-RACF) qui sera utilisable entre un réseau visité et un réseau d'attache intra-domaine ou inter-domaines ;
- création des messages de négociation de ressources ;
- création des messages pour la mise à jour dynamique des ressources en fonction des modifications du profil de l'usager.

Interface inter-RACS

Le RACS doit avoir une idée en tout temps de l'emplacement de l'usager ainsi que du RACS qui lui est associé. Pour ce faire, lors de la connexion de l'usager et du téléchargement du profil, le RACS doit mémoriser l'ID de l'usager, son attache, le domaine actuel, le RACS courant et le profil négocié dans un base de données locale au RACS. Nous proposons donc la création d'un nouveau noeud dans l'architecture du RACS : le RACF. Il servira de lien entre les différents domaines et contiendra la base de données. Il aura comme rôle de rediriger les requêtes de réservation de ressources au bon A-RACF dans le même domaine ou dans un domaine distinct. Nous proposons aussi la création des nœuds suivants :

- I-RACF (RACF global dans le réseau d'attache) ;
- S-RACF ou V-RACF (RACF dans le réseau visité) ;
- P-RACF ou H-RACF (RACF d'attache).

Le Tableau 3.8 montre un exemple d'informations que le RACF devra sauvegarder sur la localisation des usagers. La ligne 1 montre un client d'attache qui est présentement connecté sur le RACF numéro 3 de Fido (domaine visité). La ligne 2 montre un client d'attache qui est présentement connecté sur le A-RACF local numéro 5. La ligne 3 montre un client de Fido (autre domaine) qui est présentement

connecté sur le A-RACF local numéro 7.

TABLEAU 3.8 Exemple d'informations sauvegardées dans la base de données

ID de l'usager	Attache de l'utilisateur	H-RACF d'attache	Domaine actuel	RACF actuel	A-RACF actuel	Profil	Ress
1231001	local	S/O	fido.com	racf3. fido.com	S/O	[profil négocié]	
1456789	local	S/O	local	S/O	aracf5	[profil]	
4567893	fido.com	racf45. fido.com	local	S/O	aracf7	[profil négocié]	

Le champ *ID de l'utilisateur* représente l'identificateur, qui est unique à un domaine, de l'usager. Le champ *Attache de l'utilisateur* représente le réseau d'attache de l'usager. Le *H-RACF d'attache* est le H-RACF qu'il faut informer des réservations quand l'utilisateur est en visite dans un autre réseau. Le champ *Domaine actuel* enregistre le domaine dans lequel l'utilisateur est présentement connecté. Ce champ est utile pour le système P-X, I-X et S-X. Le *RACF actuel* sauvegarde le RACF qui est présentement utilisé par l'usager. Le *A-RACF actuel* est utile lorsque l'usager est local au réseau et sauvegarde le A-RACF utilisé présentement par l'usager. Le champ *profil* sauvegarde le profil négocié lorsque deux domaines sont impliqués (usager en déplacement) et brute lorsque seulement un domaine est impliqué (usager dans son réseau d'attache). Le champ Ress contient les réservations actives de l'usagers. Les informations qui y sont contenues sont transférées au CDCF (si l'usager est dans son domaine d'attache) ou au H-RACF (s'il est en visite). Il est important de noter qu'il serait possible de compresser les informations des différentes colonnes, car elles ne sont pas toutes utilisées en même temps. Cependant, ce n'est pas le but de ce projet et cette question devra être étudiée ultérieurement dans la phase d'implémentation.

La Figure 3.10 montre la nouvelle architecture du RACS. Premièrement, puisque le contrôle des services dépend du profil de l'usager et que le SPDF n'est pas au courant des profils, l'interface *Ia* qui contrôle le BGF devra être déplacée entre le A-RACF et le BGF. Deuxièmement, le noeud RACF est créé et il doit être connecté aux noeud suivants :

- le NASS, pour pouvoir avoir accès à la localisation physique des utilisateurs locaux et pour échanger les profils de ces même usagers ;
- le SPDF, pour pouvoir traiter les requêtes qui viennent du AF ainsi que pour appliquer les politiques du domaine ;
- le PDBF, pour pouvoir avoir accès aux profils de QdS et de contrôle de services des usagers ;
- les différents A-RACF locaux ou visités, pour pouvoir rediriger les requêtes de réservation de ressources ou pour informer le RACF d'attache des réservations effectuées (en utilisant l'interface *YY* inter-domaines ou intra-domaine).

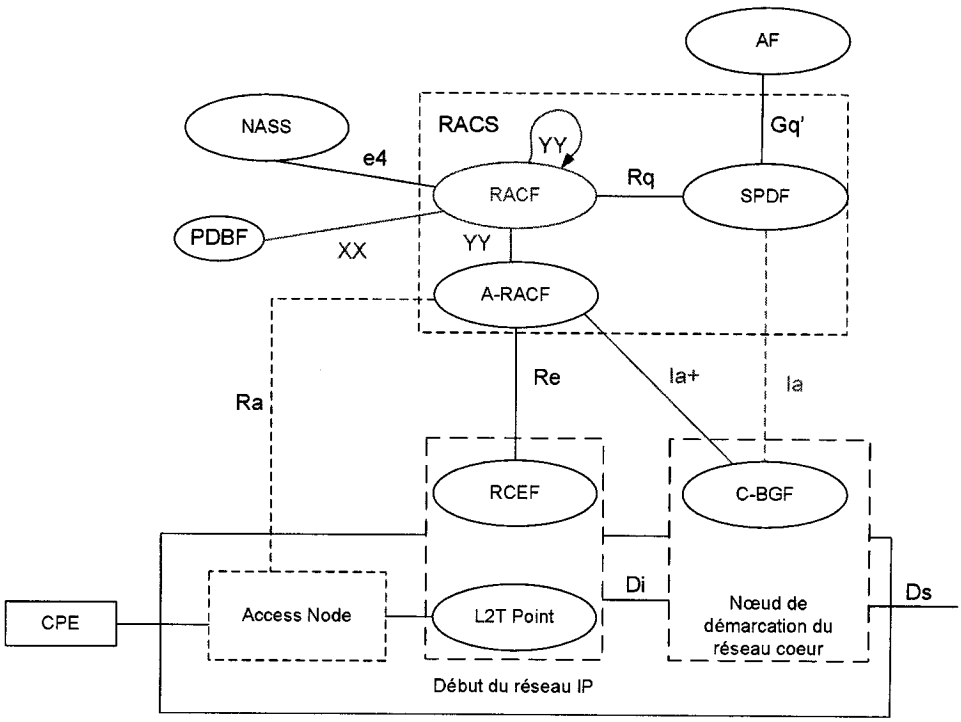

FIGURE 3.10 Architecture du RACS modifiée

Il est important de noter que le rôle fonctionnel du nœud RACF peut être implémenté distinctement ou à même le SPDF.

Négociation de ressources

Le RACS d'attache doit avoir une vision réaliste des ressources utilisées par le client dans le réseau visité. Il doit donc être informé par le RACS visité des

réservation effectuées. De plus, le RACS d'attache doit pouvoir demander des ressources au RACS visité en agissant comme un *proxy* entre les requêtes de ressources et le RACS visité.

Il doit donc y exister deux sortes de messages :

1. un *ressources-ASK* transmis par le H-RACF en mode *proxy* ;
2. un *ressources-INFORM* transmis par le V-RACF pour informer le H-RACF des réservations.

La Figure 3.11 montre une demande de ressources avec l'architecture modifiée dans le scénario où un utilisateur est dans un réseau visité. Voici les étapes de la requête :

1. l'usager demande un service de son réseau d'attache au P-CSCF ;
2. la requête est transmise au I-CSCF qui, lui, doit rediriger la requête au bon S-CSCF en passant par le I-CSCF du domaine d'attache ;
3. le S-CSCF génère une requête de réservation de ressources en fonction du profil de l'usager qui est disponible sur le H-CLF (agit en *proxy* pour avoir accès au profil synchronisé sur le V-CLF) ;
4. la requête est transmise au SPDF du H-RACS et elle est rejetée ou acceptée selon les règles locales du domaine ;
5. la requête est ensuite transmise au H-RACF ;
6. le H-RACF trouve l'usager dans sa table et agit en mode *proxy* puisque l'usager est en visite dans un autre domaine ;
7. la requête est donc transmise au I-RACF du domaine d'attache qui la transmet au I-RACF du domaine visité qui, lui, trouve le bon V-RACF ;
8. le V-RACF effectue les réservations et les configurations nécessaires ;
9. le V-RACF envoie un message d'information sur les réservations effectuées au I-RACF qui lui la transmet au I-RACF du domaine d'attache ;
10. le I-RACF d'attache redirige la requête au bon H-RACF ;
11. le H-RACF informe le S-CSCF que la réservation a été effectuée ;
12. le S-CSCF informe le P-CSCF en passant par le I-CSCF du domaine d'attache et le I-CSCF du domaine visité ;
13. le P-CSCF informe l'usager que la réservation a été effectuée pour son service.

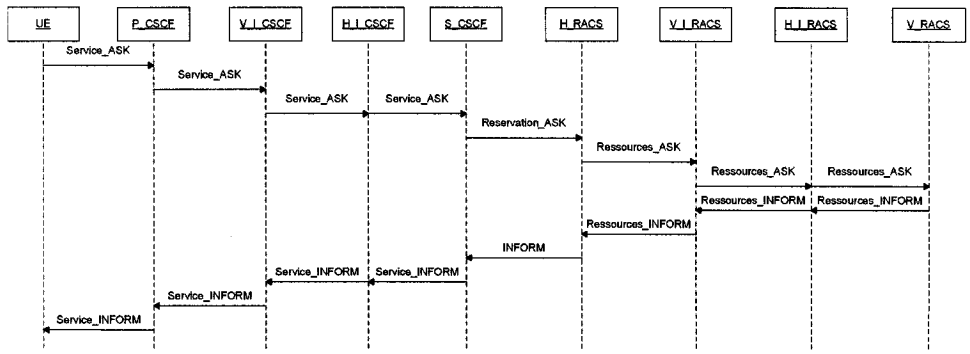

FIGURE 3.11 Demande de ressources dans l'architecture modifiée

Mise à jour dynamique des ressources

Le RACS doit être capable de modifier dynamiquement des réservations. Cela implique de refaire la synchronisation du profil de QdS et de contrôle des services entre le RACS d'attache et celui visité si l'un des deux domaines change le profil de l'usager ou le profil de ses politiques de domaine. Ce mécanisme est déjà inclus dans le volet 2 de la solution avec la création des messages de re-synchronisation.

La Figure 3.12 montre la modification du profil de QdS et de contrôle des services dans le réseau d'attache. Voici les étapes de la re-synchronisation qui en résultent :

1. le H-NASS informe le H-RACS (H-RACF) que le profil a été modifié ;
2. le H-RACF refait seulement la synchronisation de la partie du profil modifié avec le message de re-synchronisation ;
3. des messages sont échangés tant que les deux parties n'ont pas accepté le profil ;
4. la re-synchronisation se termine par l'échange des messages d'acceptation (*OK*) dans les deux directions ;
5. le V-RACS peut optionnellement informer le V-CLF du V-NASS ;
6. le V-CLF peut aussi optionnellement informer le H-CLF qui sert de *proxy*.

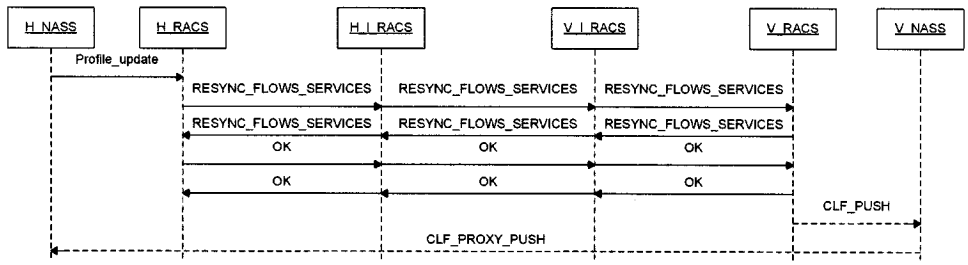

FIGURE 3.12 Modification du profil QdS et contrôle des services

3.3.3 Volet 3

Le volet 3 implique l'échange d'informations pour facturer adéquatement l'usager. Il existe plusieurs types de facturation parmi lesquelles on peut citer :

- la facturation par contenu ;
- la facturation par réservation ;
- la facturation par quantité.

Nous devons donc être capables de gérer ces trois types de facturation et ce, même lorsque l'usager utilise un réseau d'accès visité. Il faut que les informations sur les réservations effectuées, sur les quantités de ressources consommées et sur le contenu généré et reçu soient envoyées en temps réel (*online charging*) ou de manière différée (*offline charging*) au réseau d'attache. Un article (Ghys et Vaaraniemi, 2002) ébauche les différents échanges d'information pour synchroniser la facturation dans un réseau NGN multimédia.

Facturation par réservation

Les informations sur les réservations effectuées seront transmises au RACS d'attache automatiquement par le RACS visité, tel qu'abordé dans le volet 2 de la solution. Le RACS d'attache peut ensuite communiquer les informations au CDCF (*Charging and Data Collection Function*) local.

Facturation par contenu

La facturation par contenu découle des informations présentes dans le réseau visité. Elles sont générées par certaines options de contrôle des services qui peuvent enclencher un filtrage par contenu et ainsi rendre disponible un résumé du nombre de paquets et du temps d'utilisation des communications d'un usager. Nous proposons

un système P-X, I-X et S-X pour le CDCF. Avec ce système le AES et/ou le BES pourront transmettre leurs informations plus aisément au domaine d'attache.

La Figure 3.13 montre l'architecture du système avec un noeud *Proxy*, un noeud *Interrogating* et un noeud *Serving* pour la gestion des informations dans le but de contrôler la facturation dans le CDCF d'attache.

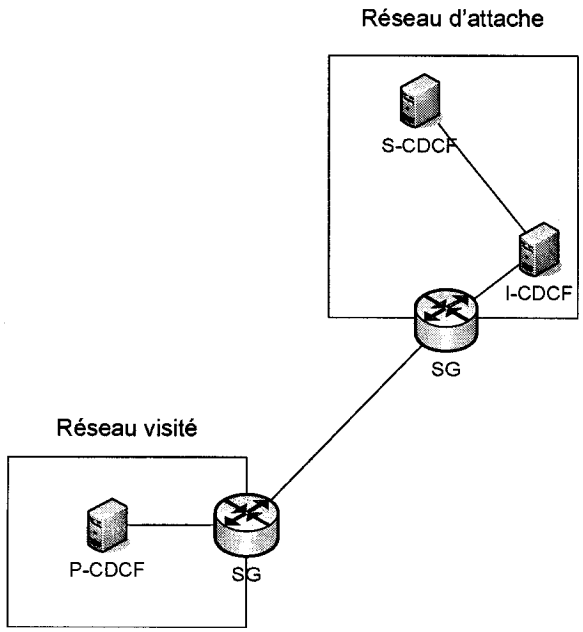

FIGURE 3.13 Architecture du système I-X pour le CDCF

Facturation par quantité

Les informations sur la facturation par quantité sont générées à partir de deux entités :

1. par le IMS d'attache, puisqu'il voit la signalisation des communications ;
2. par le AES et/ou le BES du réseau visité.

Le AES et/ou le BEs du réseau visité peuvent compter le nombre de paquets et transmettre un résumé au S-CDCF (H-CDCF) par l'intermédiaire du P-CDCF dans le domaine visité et du I-CDCF dans le réseau d'attache.

L'interface entre l'IMS d'attache et le CDCF est déjà définie par le groupe 3GPP.

Modification du profil pour la facturation

Nous proposons d'ajouter dans le profil de QdS et de contrôle des services un champ qui spécifie le type de facturation : *online chargning* ou *offline charging* et un autre champ qui spécifie l'intervalle de temps entre chaque transmission d'informations sur le résumé des communications.

Le Tableau 3.9 montre les modifications du profil de QdS et de contrôle des services pour un meilleur support de la facturation inter-domaines et intra-domaine. L'ajout du type de facturation ainsi que l'ajout de l'intervalle d'envoi des informations ont été effectués.

TABLEAU 3.9 Modification du profil pour la facturation

Profil de QdS	
- Classe de service de transport	La classe de service de transport souscrite par l'usager.
- Bande passante souscrite en amont	La quantité maximale de bande passante souscrite par l'usager en amont.
- Bande passante souscrite en aval	La quantité maximale de bande passante souscrite par l'usager en aval.
- Types de flots supportés	Vidéo, audio, data, etc.
- Différents types de flot	Bande passante souscrite en amont
	Bande passante souscrite en aval
	Priorité maximale pour la réservation
	Classe de service de transport (premium, normal, etc.)
	Les Ids des classes d'applications
Configuration initiale des grilles	
- Liste des destinations permises	La liste des adresses de destination par défaut, des ports, des préfixes et des intervalles de ports auquels du trafic peut être envoyé.
- Bande passante par défaut en amont	La quantité maximale de bande passante qui peut être utilisée sans autorisation explicite en amont.
- Bande passante par défaut en aval	La quantité maximale de bande passante qui peut être utilisée sans autorisation explicite en aval.
Configuration initiale du contrôle des services (Optionel)	
ID type de contrôle	Nombre d'argument(s)
Argument 1	Argument 2
...	
...	...
Type de facturation	Facturation en temps réel ou en différé
Intervalle d'envoi des informations	Intervalle de temps entre chaque envoi d'informations de facturation

Dans les travaux de recherche futurs, on retrouve les aspects de mobilité intra-domaine (changement d'AN, changement d'AES et changement de BES). Des mé-

canismes de gestion de mobilité rapides devraient être abordés pour ne pas être obligé de télécharger à nouveau et de re-synchroniser les profils. Cela est possible lors des changements d'AN et d'AES et on peut utiliser un pointeur de redirection pour un changement de BES intra-opérateur. La seule opération qui demandera la re-négociation complète avec le réseau d'attache est le déplacement inter-opérateurs.

Du point de vue de l'implémentation, il faudra définir plus précisément le contenu des différents messages. De plus, il faudra évaluer comment séparer les différentes options de contrôle des services entre l'AES et le BES. Est-ce mieux de répartir le plus de tâches possibles sur les différents AES (environnement réparti) ou de les centraliser sur le BES (environnement centralisé). Il est possible que la réponse à cette question ne soit pas la même pour toutes les implémentations...

CHAPITRE 4

ANALYSE DE PERFORMANCE

Dans le chapitre précédent, nous avons proposé une architecture ainsi qu'un protocole pour permettre à l'opérateur d'attache de contrôler les ressources, les services et la facturation d'un usager qui utilise son réseau d'accès ou le réseau d'accès d'un autre opérateur. Dans ce chapitre, nous reprendrons chacun des éléments de la solution proposée dans une section distincte et nous y ferons leur analyse de performance. Pour effectuer l'analyse de performance de chacun des éléments, les techniques suivantes seront utilisées dinstictement ou conjointement :

- une validation formelle avec le logiciel UPPAAL (version 3.4.11) développé à l'Université Aalborg au Danemark (*http ://www.uppaal.com*) ;
- un modèle analytique pour évaluer les délais ;
- une prévision de la taille des données à transmettre pour évaluer les délais.

Puisque dans le chapitre précédent la solution a été séparée en trois volets, les sections du présent chapitre seront divisées de la même façon pour assurer une correspondance directe entre les deux chapitres.

4.1 Volet 1

Dans cette section, nous effectuerons l'analyse de performance du volet 1 de la solution qui a été présentée au chapitre précédent. Le présent volet aborde principalement les modifications effectuées aux profils ainsi que les processus d'échange.

4.1.1 Segmentation du profil réseau en deux parties

Il a été proposé de segmenter le profil réseau, introduit par le TISPAN, en deux parties :

1. une pour l'accès ;
2. une pour la QdS et le contrôle des services.

Cette division permet de rendre les processus d'échange et de synchronisation plus dynamiques et flexibles, car chacune des parties du profil initial est liée à une section différente du réseau. Pour cette section, aucune évaluation de performance n'est nécessaire, car aucun changement n'a été effectué dans les profils qui résultent de la segmentation ou dans le processus de communication. Il existe cependant un point important à faire ressortir : puisque les profils ne seront pas échangés en même temps, le réseau ne sera pas dans le même état. Il y a donc les trois possibilités suivantes pour le deuxième envoi :

1. le réseau est plus surchargé ;
2. le réseau est moins surchargé ;
3. le réseau est identiquement surchargé.

Puisque nous ne pouvons pas prévoir l'état du réseau, nous attribuons une probabilité égale que le réseau soit plus surchargé ou qu'il le soit moins. Le fait de segmenter le profil ne devrait donc avoir aucune influence, car dans certains cas, le réseau sera plus surchargé avec la probabilité suivante :

$$\text{P(être plus surchargé)} = [1 - \text{P(de rester dans le même état)}] \,/\, 2 = [1 - 0] \,/\, 2 = 1/2$$

ou moins surchargé avec la même probabilité pour le deuxième envoi. Il est important de noter que le pourcentage de rester dans un état identique au premier envoi est quasiment nul (probabilités continues). Nous pouvons donc dire qu'il y a un pourcentage égal que le réseau soit plus surchargé ou qu'il le soit moins (50% d'être plus surchargé et 50% de l'être moins). Par conséquent, en moyenne, le réseau sera également surchargé lors du deuxième envoi que lors du premier (le même nombre de fois plus surchargé que moins surchargé). Nous posons comme hypothèse que la surcharge moyenne est égale à la diminution de charge moyenne. Ceci nous permet de conclure que deux envois sont équivalents à un seul envoi au moment du premier envoi. Cependant, les deux envois seront décalés d'un Δ_{t1}. Cela n'a pas une grande importance puisque, de toute façon, lorsque le profil était envoyé en un seul envoi, la partie qui devait être transmise à l'autre section du réseau l'était avec un Δ_{t2}. Nous supposons qu'en moyenne le Δ_{t1} est plus petit que le Δ_{t2}, car le profil QdS et contrôle des services (deuxième envoi) est envoyé avant la fin des opérations qui utilisent les données du profil d'accès. Lorsqu'il s'agissait d'un seul envoi, la partie du profil réseau contenant la QdS était seulement échangée à l'autre section

du réseau lorsque les opérations qui utilisent les données d'accès de l'ancien profil réseau étaient terminées. Il faut cependant noter que si les délais réseaux sont très grands, le Δ_{t1} pourrait devenir plus grand que le Δ_{t2} et, dans ce cas-là, la division du profil pourrait engendrer des délais supplémentaires dans le processus.

4.1.2 Ajout d'informations dans le profil d'accès

Il a été proposé d'ajouter une clé ou un identifiant privé pour authentifier l'usager dans le profil d'accès. Cela pourrait être une clé statique privée ou une clé publique (certificat). Nous ne rentrerons pas ici dans les détails des différents protocoles d'authentification. Nous supposons que la taille de la clé ou de l'identifiant peut grandement varier de 56 bits à 4096 bits et même plus. Si on suppose que le profil d'accès, présenté au Tableau 4.1, comporte les champs suivants :

a) le ID de l'abonné : supposons sa taille de 32 bits ($2^{32} = 4294967296$) ;

b) l'indicateur privé : supposons 8 bits (le minimum pour être aligné sur des octets) ;

c) l'indicateur privé : supposons 8 bits pour le type et de 56 bits à 4096 bits pour l'identifiant ;

d) l'adresse IP assignée : supposons 128 bits (IPv6) ;

e) le domaine d'adressage : supposons un maximum de 128 caractères ascii ($128 * 8bits/caract = 1024bits$).

TABLEAU 4.1 Différentes sections du profil d'accès modifié

Éléments d'information	**Description**
ID de l'abonné	L'identité de l'abonné qui demande une connectivité IP
Indicateur privé	Indique si les informations de localisation peuvent être exportées à la couche des services et des applications
Clé ou identifiant de l'usager	Information pour authentifier l'usager
Adresse globale unique	
- L'adresse IP assignée	L'adresse IP du *Home Agent* (HA)
- Domaine d'adressage	Le domaine d'adressage dans lequel l'adresse est valide et significative

Au minimum, l'ajout d'un champ identifiant de 64 bits (implique le type de 8 bits et l'identifiant de 56 bits) augmente la taille des données de 5,37%.

$$((1256bits - 1192bits)/1192bits) * 100\% = 5,37\%$$

Au maximum, l'ajout d'un champ identifiant de 4104 bits (implique le type de 8 bits et l'identifiant de 4096 bits) augmente la taille des données de 344,30%.

$$((5296bits - 1192bits)/1192bits) * 100\% = 344,30\%$$

Ainsi, il en résulte une influence non-négligeable sur la taille du profil puisque sa taille initiale est petite. Cela aura donc une répercussion sur le délai de transmission. Nous supposons que les délais de traitement, de propagation ($distance * 5\mu s/km$) et d'attente (longueur du tampon * % d'utilisation / capacité) ne dépendent pas de la longueur des paquets. Le délai de transmission est donné par la formule suivante :

$$Delai{=}Longueur/Capacite$$

On suppose des liens ayant des capacités de 1 Mbps (1 000 000 bits/s). Donc, avec un identifiant de 64 bits, la différence de délai est de 64 μs :

$$1256bits/1Mbps - 1192bits/1Mbps = 64\mu s$$

et avec un identifiant de 4104 bits, la différence de délai est de 4.104 ms :

$$5296bits/1Mbps - 1192bits/1Mbps = 4104\mu s = 4.104ms$$

Nous pouvons conclure qu'une clé de grande taille augmentera de façon considérable le délai de transmission, mais puisque nous pouvons nous permettre quelques secondes de configuration lorsqu'un usager entre dans un nouveau réseau, ce délai supplémentaire devient acceptable. Il est aussi intéressant de noter que si un protocole de type XML était utilisé, il faudra rajouter la taille des balises dans les calculs. Dans le cas d'un protocole standard (non-XML), des informations sur la longueur des champs variables devraient être rajoutées et donc incluses dans les calculs.

4.1.3 Ajout d'informations pour la QdS et le contrôle des services

La seconde partie, résultante de la segmentation de l'ancien profil réseau, introduit par le TISPAN, est transformée en un profil consacré à la QdS et au contrôle des services. Plusieurs informations ont été modifiées ou ajoutées à ce profil. Parmi celles-ci, on retrouve les informations de QdS par type de flot et celles pour la configuration initiale du contrôle des services. Nous supposons que le profil de Qds et de contrôle des services, présenté au Tableau 4.2, comporte les champs suivants :

Section du profil de Qds :

a) la classe de service de transport : supposons 8 bits (puisque les 3 bits de DiffServ (Blake *et al.*, 1998) ne semblent pas suffire) ;

b) la bande passante souscrite en amont : supposons 16 bits (maximum de 512 Mbps)

$$2^{16} kbytes/s = 65536 kbytes/s * \frac{1 Mbytes/s}{1024 kbytes/Mbytes} * (8 bits/bytes) = 512 Mbps$$

$$= 512000000 bits/s = 512 Mbps$$

c) la bande passante souscrite en aval : supposons 16 bits (maximum de 512 Mbps) ;

d) les types de flots supportés : supposons un champ variable d'un maximum de 128 caractères ascii ($128 caract * 8 bits/caract = 1024 bits$) avec une moyenne de 16 caractères ($16 caract * 8 bits/caract = 128 bits$) [video,audio,data] ;

e) les informations sur les différents types de flots (moyenne de 3 types de flots sur 16 caractères [video,audio,data]) :
   - la bande passante souscrite en amont : supposons 16 bits (maximum de 512 Mbps) ;
   - la bande passante souscrite en aval : supposons 16 bits (maximum de 512 Mbps) ;
   - la priorité maximale pour la réservation : supposons 8 bits (256 priorités) ;
   - la classe de service de transport : supposons 8 bits (256 classes) ;
   - les Ids des classes d'applications : supposons un champ variable de 128 caractères ascii ($128 caract * 8 bits/caract = 1024 bits$) avec une moyenne de 0 caractère (aucune restriction d'application).

Section de la configuration initiale des grilles :

a) la liste des destinations permises : supposons un champ variable d'un maximum de 1024 caractères ascii ($1024 caract * 8 bits/caract = 8192 bits$) avec une moyenne de 0 caractère (aucune restriction de destination) ;

b) la bande passante par défaut en amont : supposons 16 bits (maximum de 512 Mbps) ;

c) la bande passante par défaut en aval : supposons 16 bits (maximum de 512 Mbps) ;

Section de la configuration initiale du contrôle des services (supposons une moyenne de trois contrôles) :

a) le Id du type de contrôle : supposons 16 bits ($2^{16} = 65536$ types) ;

b) le nombre d'argument(s) : supposons 8 bits ($2^8 = 256$ arguments) ;

c) chacun des arguments (moyenne de 2) : supposons un champ variable entre 8 bits (ou un caractère) et 1024 bits (128 caractères) avec une moyenne de 64 bits (ou 8 caractères).

La taille moyenne du profil avant les modifications, présenté au Tableau 4.3, était de 80 bits et la nouvelle taille moyenne après les modifications est de 648 bits. La modification représente donc, en moyenne, une augmentation de 568 bits, soit de 710,00% :

$$(648 bits - 80 bits)/80 bits * 100\% = 710,00\%$$

Lorsque le profil a sa taille minimale, c'est-à-dire aucun type de flot supporté et aucun contrôle des services, l'ancien profil reste à 80 bits et le nouveau profil descends à 72 bits, soit une diminution de 10,00% :

$$(80 bits - 72 bits)/80 bits * 100\% = 10,00\%$$

Par contre, lorsque le nombre de flots supportés et le nombre de contrôles des services est très grand, la taille est elle aussi très grande. Supposons maintenant un exemple avec tous les champs variables à leur taille maximale. Cela représente donc 24 types de flots et 10 options de contrôle des services (chacun ayant 4 arguments de taille maximale). L'ancien profil augmente à 9296 bits et le nouveau à 75320 bits, donc une augmentation de 710,24% :

TABLEAU 4.2 Différentes sections du profil de QdS et de contrôle des services

Profil de QdS	
- Classe de service de transport	La classe de service de transport souscrite par l'usager.
- Bande passante souscrite en amont	La quantité maximale de bande passante souscrite par l'usager en amont.
- Bande passante souscrite en aval	La quantité maximale de bande passante souscrite par l'usager en aval.
- Types de flots supportés	Vidéo, audio, data, etc.
- Différents types de flot	Bande passante souscrite en amont
	Bande passante souscrite en aval
	Priorité maximale pour la réservation
	Classe de service de transport (premium, normal, etc.)
	Les Ids des classes d'applications
Configuration initiale des grilles	
- Liste des destinations permises	La liste des adresses de destination par défaut, des ports, des préfixes et des intervalles de ports auquels du trafic peut être envoyé.
- Bande passante par défaut en amont	La quantité maximale de bande passante qui peut être utilisée sans autorisation explicite en amont.
- Bande passante par défaut en aval	La quantité maximale de bande passante qui peut être utilisée sans autorisation explicite en aval.
Configuration initiale du contrôle des services (Optionel)	
ID type de contrôle	Nombre d'argument(s)
Argument 1	Argument 2
...	
...	...

$$(75320bits - 9296bits)/9296bits * 100\% = 710,24\%$$

Il existe donc une influence non-négligeable sur la taille du profil puisque la quantité d'options ajoutées est grande. Cela aura donc une répercussion sur le délai de transmission. Nous supposons que les délais de traitement, de propagation ($distance * 5\mu s/km$) et d'attente (longueur du tampon * % d'utilisation / capacité) ne dépendent pas de la longueur des paquets. Le délai de transmission est donné par la formule suivante :

$$Delai=Longueur/Capacite$$

On suppose des liens ayant des capacités de 1 Mbps (1 000 000 bits/s). Donc, avec

TABLEAU 4.3 Profil réseau sans modification

Profil de QdS	
- Classe de service de transport	La classe de service de transport souscrite par l'usager.
- Bande passante souscrite en amont	La quantité maximale de bande passante souscrite par l'usager en amont.
- Bande passante souscrite en aval	La quantité maximale de bande passante souscrite par l'usager en aval.
- Priorité maximale	La priorité maximale allouée pour une requête de réservation.
- Les Ids des classes d'applications	Identifie les classes d'applications allouées pour utiliser le profil de QdS.
Configuration initiale des grilles	
- Liste des destinations permises	La liste des adresses de destination par défaut, des ports, des préfixes et des intervalles de ports auquels du trafic peut être envoyé.
- Bande passante par défaut en amont	La quantité maximale de bande passante qui peut être utilisée sans autorisation explicite en amont.
- Bande passante par défaut en aval	La quantité maximale de bande passante qui peut être utilisée sans autorisation explicite en aval.

la taille moyenne, la différence de délai est de 568 μs :

$$648bits/1Mbps - 80bits/1Mbps = 568\mu s$$

Avec la taille inférieure, la différence de délai est de -8 μs :

$$72bits/1Mbps - 80bits/1Mbps = 4104\mu s = -8\mu s$$

Avec la taille supérieure, la différence de délai est de 66,02 ms :

$$75320bits/1Mbps - 9296bits/1Mbps = 4104\mu s = 66,02ms$$

Nous pouvons donc conclure que le fait de rajouter des options de QdS et de contrôle des services augmentera de façon considérable le délai de transmission. Cependant, le résultat de cette augmentation est facilement compensable par l'ajout de nombreuses fonctionnalités et la grande augmentation de flexibilité. Un fait à noter : nous pouvons nous permettre un délai de quelques secondes pour la configuration d'un nouvel usager qui entre dans un réseau. Il est aussi intéressant de constater que si un protocole de type XML était utilisé, il faudrait rajouter la taille des balises

dans les calculs. Dans le cas d'un protocole standard (non-XML), des informations sur la longueur des champs variables devraient être rajoutées et donc incluses dans les calculs.

4.1.4 Échange des profils

Avant les modifications

Dans cette sous-section, le processus original d'échange et de synchronisation du profil entre le réseau d'attache et le réseau visité sera analysé. Nous étudierons ce processus à l'aide d'un modèle analytique et d'une validation formelle. La Figure 4.1 montre le diagramme de séquence pour l'échange du profil avant les modifications effectuées dans ce projet.

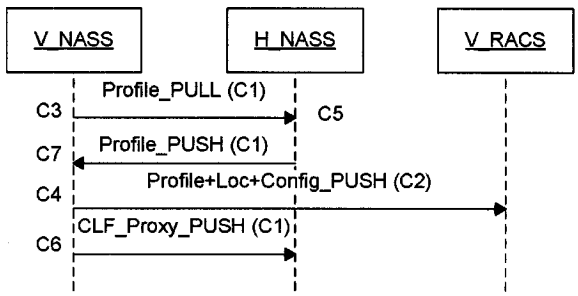

FIGURE 4.1 Diagramme de séquence de téléchargement du profil avant les modifications

Nous en déduirons un modèle analytique qui permettra de comparer les performances de ce modèle avec celui modifié. Nous supposons les coûts symétriques et nous commençons pas définir les variables utilisées dans ce modèle :

$C_{V-NASS-H-NASS}$	C_1	Coût de transport entre le V-NASS du domaine visité et le H-NASS du domaine d'attache.
$C_{V-NASS-V-RACS}$	C_2	Coût de transport entre le V-NASS du domaine visité et le V-RACS du domaine visité.
$C_{NASS_{Profile-ASK}}$	C_3	Coût de la préparation de la demande du profil.
$C_{NASS_{Profile-SEND}}$	C_4	Coût de la préparation de l'envoi du profil avec la confirmation de la configuration de l'accès.
$C_{NASS_{Profile-PULL}}$	C_5	Coût pour la recherche du profil de l'usager par le NASS ou le RACS.

$C_{NASS_{Proxy-PUSH}}$	C_6	Coût de la préparation de la requête de renvoi à transmettre au H-CLF du domaine d'attache.
$C_{NASS_{Profile-PROC}}$	C_7	Coût pour configurer l'accès de l'usager.

Le processus sans modification engendre donc le modèle suivant :

$$C_3 + C_1 + C_5 + C_1 + C_7 + C_4 + C_2 + C_6 + C_1$$

$$= 3 * C_1 + C_2 + C_3 + C_4 + C_5 + C_6 + C_7$$

Nous lui fixerons des coûts et en ferons varier quelques-uns dans la prochaine sous-section et ce, dans le but de le comparer avec le modèle modifié.

Nous avons ensuite utilisé le logiciel UPPAAL pour effectuer la validation formelle du processus non-modifié. Plus précisément, nous avons créé 4 fichiers UPPAAL :

1. une version complète du processus de connexion non-modifié du mobile lorsqu'il est dans son réseau d'attache ;
2. une version simplifié du même processus ;
3. une version complète du processus de connexion non-modifié du mobile lorsqu'il est dans un réseau d'attache visité ;
4. une version simplifié du même processus.

Les fichiers précédents sont disponibles par le biais du groupe LARIM de l'École Polytechnique de Montréal.

Nous avons été obligé de créer des versions simplifiées, car il y avait explosion de la mémoire maximale par processus dans un système d'exploitation 32 bits. Le même résultat aurait été atteint avec un système d'exploitation 64 bits, car UPPAAL est un processus 32 bits. Nous avons essayé d'utiliser directement la commande de vérification d'UPPAAL *verifyta.exe* pour économiser la mémoire de l'interface graphique, mais nous avons obtenu le même dépassement. Il aurait fallu consulter un expert en *Computational Tree Logic* (CTL) et il n'y a aucune garantie que nous aurions obtenu un succès. Nous pensons que le modèle était tout simplement trop réaliste (trop près d'une implémentation). Nous avons donc créé une version simplifiée à partir de la version complète en enlevant les aspects aléatoires ainsi que les

mécanismes de retransmission et d'abandon.

Voici la liste des propriétés temporelles que nous avons testées :

- atteignabilité ;
- sûreté ;
- vivacité ;
- équité ;
- blocage.

La propriété de blocage (*A[] not deadlock*) nous permet de vérifier que le protocole ne bloquera jamais. Dans notre cas, la satisfaction de cette propriété permet de découler la satisfaction d'autres propriétés. En effet, l'atteignabilité de l'état *UE.Wait_Can_Use_Network* et de la transition *UE.AMF_Can_Use_Network* sont satisfaites, sinon nous serions en situation de blocage. La propriété de sûreté qui vérifie que le système ne passera jamais par la transition *AMF_Cannot_Use_Network* est aussi satisfaite, sinon nous serions en blocage. La vivacité qui est la propriété qu'un état finisse par se produire est aussi satisfaite, car l'état *UE.Wait_Can_Use_Network* est atteint à chaque itération. De plus, l'équité du même état est aussi assuré, car cet état sera infiniment atteint.

L'évaluation de ces mêmes propriétés dans le modèle complet n'a pas pu être effectuée, car nous avons atteint les limites de l'outil UPPAAL. Par contre, nous avons effectué une simulation sur le modèle complet avec l'aide d'une variable pour compter les succès. Il est important de noter qu'après quelques heures d'exécution, aucune erreur n'est survenue. Nous en concluons donc que le modèle complet est probablement correct.

Après les modifications

Dans cette sous-section, le processus modifié d'échange et de synchronisation du profil entre le réseau d'attache et le réseau visité sera analysé. Nous analyserons ce processus à l'aide d'un modèle analytique et à l'aide d'une validation formelle. La Figure 4.2 montre le diagramme de séquence pour l'échange du profil après les modifications effectuées dans ce projet.

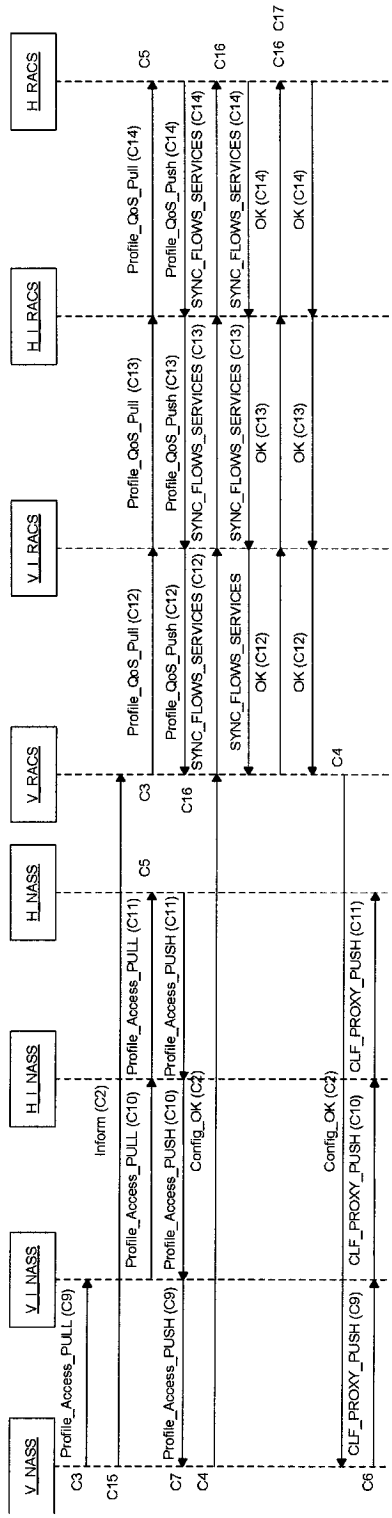

FIGURE 4.2 Diagramme de séquence modifié du téléchargement du profil

Nous en déduirons un modèle analytique qui permettra de comparer les performances de ce modèle avec celles du modèle non-modifié. Nous supposons les coûts symétriques et nous commençons pas définir les variables supplémentaires suivantes :

$C_{V-NASS-V-I-NASS}$	C_9	Coût de transport entre le V-NASS du domaine visité et le V-I-NASS du domaine visité.
$C_{V-I-NASS-H-I-NASS}$	C_{10}	Coût de transport entre le V-I-NASS du domaine visité et le H-I-NASS du domaine d'attache.
$C_{H-NASS-H-I-NASS}$	C_{11}	Coût de transport entre le H-NASS du domaine d'attache et le H-I-NASS du domaine d'attache.
$C_{V-RACS-V-I-RACS}$	C_{12}	Coût de transport entre le V-RACS du domaine visité et le V-I-RACS du domaine visité.
$C_{V-I-RACS-H-I-RACS}$	C_{13}	Coût de transport entre le V-I-RACS du domaine visité et le H-I-RACS du domaine d'attache.
$C_{H-RACS-H-I-RACS}$	C_{14}	Coût de transport entre le H-RACS du domaine d'attache et le H-I-RACS du domaine d'attache.
$C_{NASS_{Inform-RACS}}$	C_{15}	Coût de la préparation du message pour informer le RACS.
$C_{RACS_{Analyse}}$	C_{16}	Coût de l'analyse du profil de l'usager en fonction des règles locales du RACS.
$C_{RACS_{Profile-PROC}}$	C_{17}	Coût pour configurer l'accès de l'usager.

Le processus avec modifications engendre donc le modèle suivant :

$$C_3 + C_9 +$$

$$C_{15} + C_2 +$$

$$C_{10} + C_{11} + C5 + C_3 + C_{12} + C_{13} + C_{14} + C5 +$$

$$C_9 + C_{10} + C_{11} + C_7 + C_{12} + C_{13} + C_{14} + C16 +$$

$$C4 + C_2 + C_{12} + C_{13} + C_{14} + C_{16} +$$

$$C_{12} + C_{13} + C_{14} + C_{16} + C_{17} +$$

$$C_{12} + C_{13} + C_{14} +$$

$$C_{12} + C_{13} + C_{14} +$$

$$C_4 + C_2 +$$

$$C_6 + C_9 + C_{10} + C_{11}$$

$$= 3 * C_2 + 2 * C_3 + 2 * C4 + 2 * C5 + C_6 + C_7 + 3 * C_9 + 3 * C_{10}$$

$$+3 * C_{11} + 6 * C_{12} + 6 * C_{13} + 6 * C_{14} + C_{15} + 3 * C_{16} + C_{17}$$

Nous effectuons les simplifications suivantes pour le rendre plus facilement comparable avec le modèle sans modification :

- $C_{V_{NASS}-H_{NASS}} = C_1 = C_9 + C_{10} + C_{11}$;
- $C_{NASS_{Profile-PROC}} = C_7 = C_{RACS_{Profile-PROC}} = C_{17}$;
- $C_{V_{RACS}-H_{RACS}} = C_{V_{NASS}-H_{NASS}} = C_1 = C_{12} + C_{13} + C_{14}$.

Avec les simplifications précédentes, le modèle avec modifications devient :

$$= 9 * C_1 + 3 * C_2 + 2 * C_3 + 2 * C4 + 2 * C5 + C_6 + 2 * C_7 + C_{15} + 3 * C_{16}$$

Nous pouvons ensuite désigner C_1 comme le $C_{INTER-DOMAINES}$ et C_2 comme le $C_{INTRA-DOMAINE}$.

Nous faisons ensuite l'hypothèse suivante :

- tous les temps de traitement ou de préparation de requête sont égaux ou inférieurs à 1 ms (réaliste avec les vitesses des processeurs actuelles).

Le modèle non-modifié devient donc :

$$C_{total-non-modifie} = 3 * C_{INTER-DOMAINES} + C_{INTRA-DOMAINE} + 5ms$$

Le modèle avec modifications devient :

$$C_{total-modifie} = 9 * C_{INTER-DOMAINES} + 3 * C_{INTRA-DOMAINE} + 13ms$$

Tout au long de ce chapitre, nous allons utiliser les constantes suivantes :

- $C_{INTRA-DOMAINE} = 10\text{ms}$;
- $C_{INTRA-DOMAINE} = 50\text{ms}$;
- $C_{ACCES} = 20$ ms ;

- $C_{INTRA-RACS} = 5$ ms $= C_{INTRA-SYSTEM}$;
- $C_{INTRA-NASS} = 5$ ms $= C_{INTRA-SYSTEM}$.

Les valeurs précédents sont considérées comme des valeurs raisonnables dans le domaine des télécommunications.

Puisque les deux modèles se réduisent maintenant à 2 variables, nous allons tracer deux graphiques :

1. un premier qui représente le coût total en temps versus $C_{INTER-DOMAINES}$ variant avec $C_{INTRA-DOMAINE}$ constant [10 ms] ;
2. un second qui représente le coût total en temps versus $C_{INTRA-DOMAINE}$ variant avec $C_{INTER-DOMAINES}$ constant [50 ms] ;

La Figure 4.3 montre le premier graphique. Nous y voyons bien l'effet du facteur 3 (9/3) supplémentaire qui multiplie $C_{INTER-DOMAINES}$ dans le modèle modifié. Pour une valeur normale de $C_{INTER-DOMAINES}$ de 50 ms, on trouve un coût total de 165 ms pour le modèle non-modifié et de 493 ms pour le modèle modifié. La différence de coût est donc très largement compensée par l'ajout des différentes fonctionnalités et des différents mécanismes. De plus, un délai de 493 ms est très acceptable lorsqu'un nouvel usager se connecte au réseau.

La Figure 4.4 montre le deuxième graphique. Nous y voyons bien l'effet du facteur 3 (3/1) supplémentaire qui multiplie $C_{INTRA-DOMAINE}$ dans le modèle modifié. Pour une valeur normale de $C_{INTRA-DOMAINE}$ de 10 ms, on retrouve les mêmes valeurs que pour la figure précédente ; soit, 165 ms pour le modèle non-modifié et 493 ms pour celui modifié. Comme pour la figure précédente, la différence de coût est donc très largement compensée par l'ajout des différentes fonctionnalités et des différents mécanismes.

Nous avons ensuite utilisé le logiciel UPPAAL pour effectuer la validation formelle du processus modifié. Plus précisément, nous avons créé 4 fichiers UPPAAL :

1. une version complète du processus modifié de connexion du mobile lorsqu'il est dans son réseau d'attache ;
2. une version simplifiée du même processus ;
3. une version complète du processus modifié de connexion du mobile lorsqu'il est dans un réseau d'attache visité ;
4. une version simplifié du même processus.

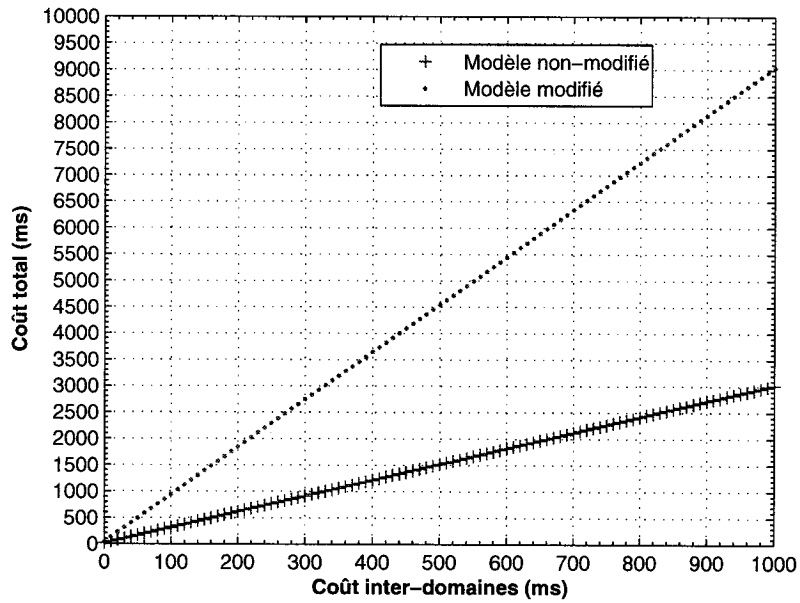

FIGURE 4.3 Coût total versus le $C_{INTER-DOMAINES}$ pour le scénario d'échange de profil

Les fichiers précédents sont disponibles par le biais du groupe LARIM de l'École Polytechnique de Montréal.

Voici la liste des propriétés temporelles que nous avons testées :

- atteignabilité ;
- sûreté ;
- vivacité ;
- équité ;
- blocage.

La propriété de blocage (*A[] not deadlock*) nous permet de vérifier que le protocole ne bloquera jamais. Dans notre cas, la satisfaction de cette propriété permet de d'établir la satisfaction d'autres propriétés. En effet, l'atteignabilité de l'état *UE.Wait_Can_Use_Network* et de la transition *UE.AMF_Can_Use_Network* est satisfaite, sinon nous serions en situation de blocage. La propriété de sûreté qui vérifie que le système ne passera jamais par la transition *AMF_Cannot_Use_Network* est aussi satisfaite sinon nous serions en blocage. La vivacité qui est la propriété qu'un état finisse par se produire est aussi satisfaite ; car, l'état *UE.Wait_Can_Use_Network*

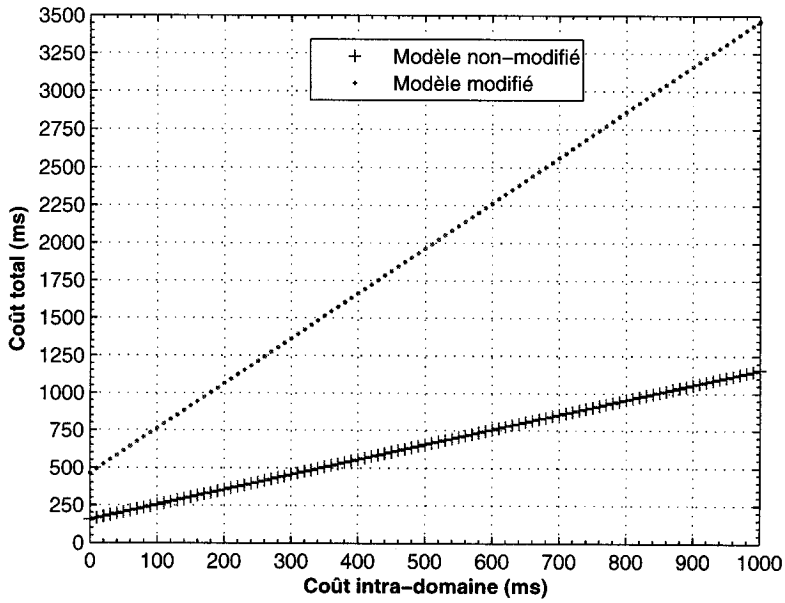

FIGURE 4.4 Coût total versus le $C_{INTRA-DOMAINE}$ pour le scénario d'échange de profil

est atteinte à chaque itération. De plus, l'équité du même état est aussi assurée, car cet état sera infiniment atteint.

L'évaluation de ces mêmes propriétés dans le modèle complet n'a pas pu être effectuée, car nous avons atteint les limites de l'outil UPPAAL. Par contre, nous avons effectué une simulation sur le modèle complet avec l'aide d'une variable incrémentale pour compter les succès. Il est important de noter qu'après quelques heures d'exécution aucune erreur n'est survenue. Nous en concluons donc que le modèle complet est probablement correct.

4.2 Volet 2

Dans cette section, nous effectuerons l'analyse de performance du volet 2 de la solution qui a été présentée au chapitre précédent. Le présent volet aborde principalement les processus de réservation de ressources. Nous allons utiliser les coûts suivants pour l'élaboration des modèles analytiques de ce volet :

C_{MN-AMF}	C_1	Coût de transport entre le MN et le AMF dans le même domaine.
$C_{AMF-RCEF}$	C_2	Coût de transport entre le AMF et le RCEF dans le même domaine.
$C_{RCEF-AF}$	C_3	Coût de transport entre le RCEF et le AF dans le même domaine.
C_{MN-AF}	C_4	Coût de transport entre le MN et le AF dans le même domaine.
C_{AF-CLF}	C_5	Coût de transport entre le AF et le CLF dans le même domaine.
$C_{AF-SPDF}$	C_6	Coût de transport entre le AF et le SPDF dans le même domaine.
$C_{SPDF-BGF}$	C_7	Coût de transport entre le SPDF et le BGF dans le même domaine.
$C_{SPDF-A-RACF}$	C_8	Coût de transport entre le SPDF et le A-RACF dans le même domaine.
$C_{A-RACF-RCEF}$	C_9	Coût de transport entre le A-RACF et le RCEF dans le même domaine.
$C_{AF-RACF}$	C_{20}	Coût de transport entre le AF et le RACF dans le même domaine.
$C_{A-RACF-BGF}$	C_{21}	Coût de transport entre le A-RACF et le BGF dans le même domaine.
$C_{RACF-A-RACF}$	C_{22}	Coût de transport entre le RACF et le A-RACF dans le même domaine.
$C_{RCEF-C-BGF}$	C_{25}	Coût de transport entre le RCEF et le C-BGF dans le même domaine.
$C_{C-BGF-BB-BGF}$	C_{26}	Coût de transport entre le C-BGF et le BB-BGF dans le même domaine.
$C_{BB-BGF-BB-BGF}$	C_{27}	Coût de transport entre le BB-BGF et le BB-BGF d'un autre domaine.
$C_{C-BGF-AF}$	C_{28}	Coût de transport entre le C-BGF et le AF dans le même domaine.
$C_{V-CLF-H-CLF}$	C_{29}	Coût de transport entre le V-CLF et le B-CLF inter-domaines.

$C_{P-CSCF-I-CSCF}$	C_{30}	Coût de transport entre le P-CSCF et le I-CSCF dans le même domaine.
$C_{V-I-CSCF-H-I-CSCF}$	C_{31}	Coût de transport entre le V-I-CSCF et le H-I-CSCF inter-domaines.
$C_{RACF-I-RACF}$	C_{32}	Coût de transport entre le RACF et le I-RACF dans le même domaine.
$C_{V-I-RACF-H-I-RACF}$	C_{33}	Coût de transport entre le V-I-RACF et le H-I-RACF inter-domaines.

$C_{MN_{APP}}$	C_{10}	Coût de la préparation de la requête d'application.
$C_{AF_{APP}}$	C_{11}	Coût de l'analyse de la requête d'application.
$C_{CLF_{LOC}}$	C_{12}	Coût de la recherche de localisation.
$C_{AF_{RESERV}}$	C_{13}	Coût de la préparation de la requête de réservation.
$C_{SPDF_{RESERV}}$	C_{14}	Coût de l'analyse de la requête de réservation.
$C_{SPDF_{CONFIG}}$	C_{15}	Coût de la préparation de la requête de configuration.
$C_{A-RACF_{CONFIG}}$	C_{16}	Coût de la configuration.
$C_{BGF_{CONFIG}}$	C_{17}	Coût de la configuration.
$C_{RCEF_{CONFIG}}$	C_{18}	Coût de la configuration.
$C_{A-RACF_{RESERV}}$	C_{19}	Coût de la préparation de la requête de configuration.
$C_{RACF_{RESERV}}$	C_{23}	Coût de l'analyse de la requête de réservation.
$C_{RACF_{CONFIG}}$	C_{24}	Coût de la préparation de la requête de configuration.
$C_{RACF_{INFORM}}$	C_{34}	Coût de la préparation de la requête d'information sur les réservations.
$C_{RACF_{SAVE}}$	C_{35}	Coût de la sauvegarde des informations sur les réservations.

Nous dressons une liste commune des coûts afin d'établir une uniformité entre les différents modèles. Nous supposons les coûts symétriques. Il est aussi important de noter que seulement les coûts de traitement et de préparation des requêtes prédominants y sont inclus. Nous avons effectué ces simplifications afin de rendre les modèles plus simples et plus compréhensibles.

4.2.1 Réservation de ressources dans le réseau d'attache avant les modifications

Dans cette sous-section, le processus original de réservation de ressources dans le réseau d'attache sera analysé. Ce sera fait à l'aide d'un modèle analytique et d'une validation formelle.

La Figure 4.5 montre le diagramme de séquence pour la réservation de ressources dans le réseau d'attache avant les modifications.

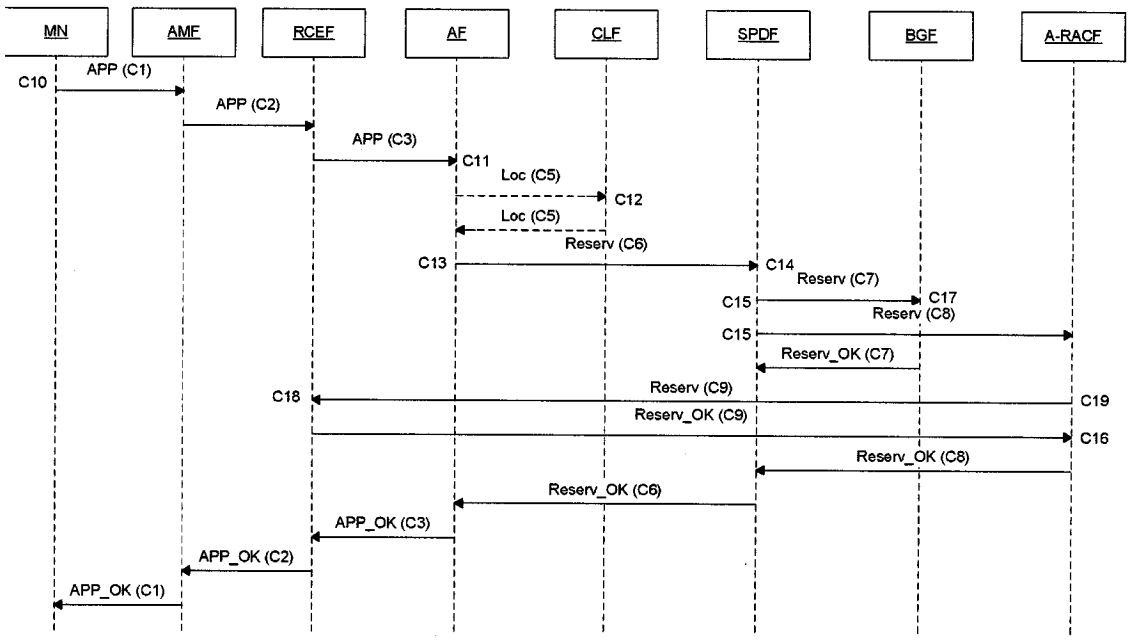

FIGURE 4.5 Scénario de réservation dans le réseau d'attache avant les modifications

Nous en déduirons un modèle analytique qui permettra de comparer ses performances avec celles du modèle modifié. Nous utiliserons la liste des variables présentée au début du Volet 2.

Le processus sans modification engendre donc le modèle suivant :

$$C_{10} + C_1 + C_2 + C_3 + C_{11} +$$

$$C_5 + C_{12} + C_5 +$$

$$C_{13} + C_6 + C_{14} +$$

$$C_{15} + C_7 + C_{15} + C_8 +$$

$$C_{17} + C_7$$

$$C_{19} + C_9 + C_{18} + C_9 + C_{16} + C_8 +$$

$$C_6 + C_3 + C_2 + C_1$$

$$= 2 * C_1 + 2 * C_2 + 2 * C_3 + 2 * C_5 + 2 * C_6 + 2 * C_7 + 2 * C_8 + 2 * C9 +$$

$$C_{10} + C_{11} + C_{12} + C_{13} + C_{14} + 2 * C_{15} + C_{16} + C_{17} + C_{18} + C_{19}$$

Nous lui fixerons des coûts et en ferons varier quelque-uns dans la section suivante dans le but de le comparer avec le modèle modifié.

Nous avons ensuite utilisé le logiciel UPPAAL pour effectuer la validation formelle du processus non-modifié afin de vérifier que le processus proposé par le TISPAN était fonctionnel. Il est important de noter que nous avons fait quelques suppositions pour définir le modèle puisque le processus n'était pas entièrement défini.

Plus précisément, nous avons créé un fichier UPPAAL contenant une version du processus original de réservation de ressources lorsque l'usager est dans son réseau d'attache. Ce fichier est disponible par le biais du groupe LARIM de l'École Polytechnique de Montréal.

La version réalisée est une version qui correspond plus à une preuve de concept qu'à un modèle complet. En effet, dans ce modèle, il n'y a aucune gestion d'exception. Le but ultime de ce modèle est de vérifier que le processus peut fonctionner sans blocage, et par le fait même dresser une liste des différents noeuds et messages impliqués dans l'axe du temps.

Nous avons seulement testé la propriété temporelle du blocage.

La propriété de blocage (*A[] not deadlock*) nous permet de vérifier que le protocole ne bloquera jamais. Dans notre cas, la satisfaction de cette propriété nous est suffisante pour prouver que le processus est bien défini, car si l'une des étapes n'avait pas fonctionné, le processus serait en blocage.

4.2.2 Réservation de ressources dans le réseau d'attache après les modifications

Dans cette sous-section, le processus modifié de réservation de ressources dans le réseau d'attache sera analysé. Ce sera fait à l'aide d'un modèle analytique et d'une validation formelle.

La Figure 4.6 montre le diagramme de séquence pour la réservation de ressources dans le réseau d'attache après les modifications.

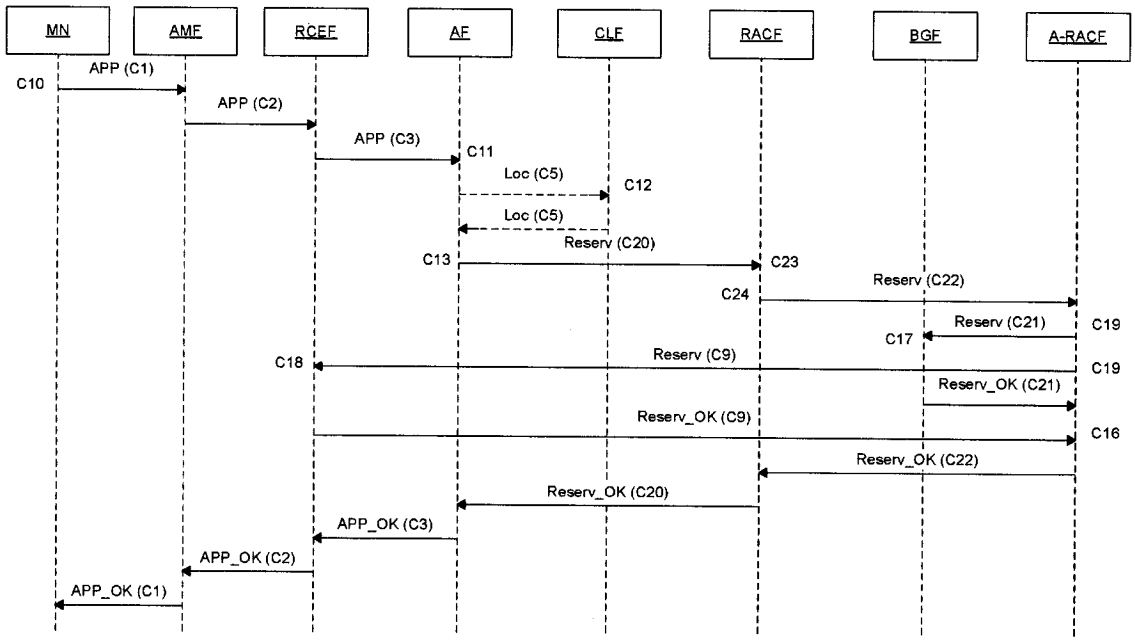

FIGURE 4.6 Scénario de réservation de ressources dans le réseau d'attache après les modifications

Nous en déduirons un modèle analytique qui permettra de comparer ses performances avec celles du modèle non-modifié qui a été présenté à la section précédente. Nous utiliserons la liste des variables présentée au début du Volet 2.

Le processus avec modifications engendre donc le modèle suivant :

$$C_{10} + C_1 + C_2 + C_3 + C_{11} +$$

$$C_5 + C_{12} + C_5 +$$

$$C_{13} + C_{20} + C_{23} +$$

$$C_{24} + C_{22} + C_{19} + C_{21} +$$

$$C_{17} + C_{21}$$

$$C_{19} + C_9 + C_{18} + C_9 + C_{16} + C_{22} +$$

$$C_6 + C_3 + C_2 + C_1$$

$$= 2 * C_1 + 2 * C_2 + 2 * C_3 + 2 * C_5 + C_6 + 2 * C_9 + C_{10} + C_{11} +$$

$$C_{12} + C_{13} + C_{16} + C_{17} + C_{18} + 2 * C_{19} + C_{20} + 2 * C_{21} +$$

$$2 * C_{22} + C_{23} + C_{24}$$

Nous faisons les hypothèses simplificatrices suivantes pour rendre plus facilement comparable les deux modèles (sans modification et avec modifications) :

- puisque la localisation est optionnelle, elle est enlevée du modèle ($C_5 = C_{12} = 0$) ;
- les temps de traitement ou de création des requêtes sont au maximum de 1 ms.

Comme dans la section précédente, nous avons supposé que les coûts de création de requête et de traitement ne dépassent pas 1 ms (réaliste avec les vitesses des processeurs actuelles).

Nous avons aussi effectué les simplifications de variables suivantes :

- $C_{MN-AF} = C_4 = C_1 + C_2 + C_3 = C_{ACCES}$;
- $C_{INTRA-RACS} = C_6 = C_7 = C_8 = C_9 = C_{20} = C_{21} = C_{22}$.

Avec les simplifications et les hypothèses simplificatrices précédentes le modèle sans modification devient :

$$C_{total-non-modifie} = 2 * C_4 + 2 * C_6 + 2 * C_7 + 2 * C_8 + 2 * C9 +$$

$$1ms + 1ms + 1ms + 1ms + 2ms + 1ms + 1ms + 1ms + 1ms$$

$$C_{total-non-modifie} = 2 * C_{ACCES} + 2 * C_6 + 2 * C_7 + 2 * C_8 + 2 * C9 + 10ms$$

$$C_{total-non-modifie} = 2 * C_{ACCES} + 8 * C_{INTRA-RACS} + 10ms$$

Avec les même simplifications, le modèle modifié devient :

$$C_{total-modifie} = 2 * C_4 + 2 * C_9 + 1ms + 1ms + 1ms + 1ms + 1ms + 1ms +$$

$$2ms + 2 * C_{20} + 2 * C_{21} + 2 * C_{22} + 1ms + 1ms$$

$$C_{total-modifie} = 2 * C_{ACCES} + 2 * C_9 + 2 * C_{20} + 2 * C_{21} + 2 * C_{22} + 10ms$$

$$C_{total-modifie} = 2 * C_{ACCES} + 8 * C_{INTRA-RACS} + 10ms$$

Il est important de noter que les 2 équations résultantes sont identiques. Cela est normal puisque nous avons seulement transféré les fonctions du nœud SPDF au RACF.

Puisque les deux modèles se réduisent maintenant à 2 variables chacun, nous allons tracer deux graphiques :

1. un premier qui représente le coût total en temps versus C_{ACCES} variant avec $C_{INTRA-RACS}$ fixé à 5 ms ;
2. un second qui représente le coût total en temps versus $C_{INTRA-RACS}$ variant avec C_{ACCES} fixé à 20 ms.

La Figure 4.7 montre le premier graphique. Nous y voyons bien que le coût total des modèles augmente deux fois plus vite que le coût d'accès (C_{ACCES}). Il est important de noter que le nombre de points a été réduit afin de visualiser la superposition des deux courbes. Pour une valeur normale de C_{ACCES} de 20 ms, on trouve un coût total de 90 ms pour les deux modèles. Il n'y a donc aucune différence au niveau du délai. Il est intéressant de noter qu'un délai de 90 ms pour effectuer la réservation des ressources est très acceptable.

La Figure 4.8 montre le deuxième graphique. Nous y voyons bien que le coût total des modèles augmente huit fois plus vite que le coût de communication intra-RACS ($C_{INTRA-RACS}$). Il est important de noter que le nombre de points a été

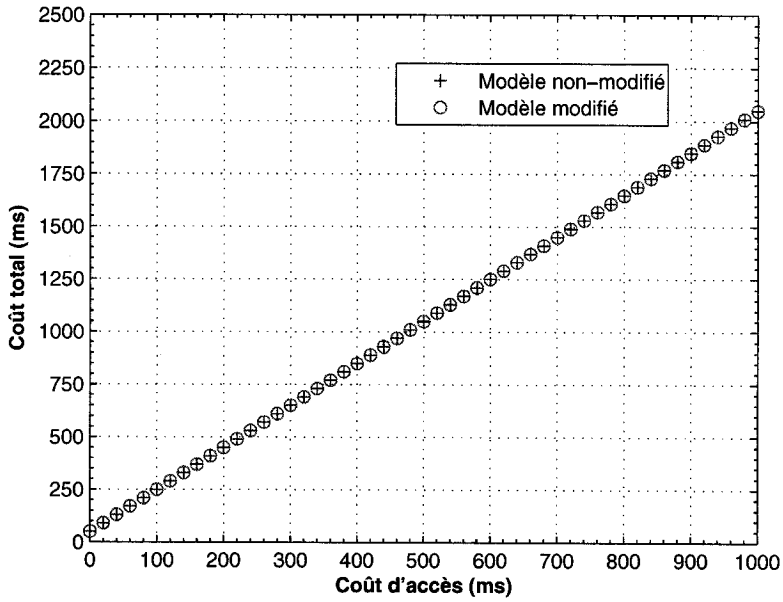

FIGURE 4.7 Coût total versus le C_{ACCES} du scénario de réservation de ressources intra-domaine

réduit afin de visualiser la superposition des deux courbes. Pour une valeur normale de $C_{INTRA-RACS}$ de 5 ms, on trouve encore un coût total de 90 ms pour les deux modèles. Il faut cependant s'assurer que les délais intra-RACS restent petits, car ils font augmenter considérablement le coût total (facteur multiplicatif élevé). Le fait de garder les délais intra-RACS petits est cependant faisable, puisque ces délais sont à l'intérieur même d'un sous-système.

Nous avons ensuite utilisé le logiciel UPPAAL pour effectuer la validation formelle du processus modifié. Plus précisément, nous avons créé un fichier UPPAAL du processus modifié de réservation de ressources lorsque l'usager est dans son réseau d'attache. Ce fichier est disponible par le biais du groupe LARIM de l'École Polytechnique de Montréal.

La version réalisée est une version qui correspond plus à une preuve de concept qu'à un modèle complet. En effet, dans ce modèle, il y a aucune gestion d'exception. Le but ultime de ce modèle est de vérifier que le processus peut fonctionner sans blocage, et par le fait même dresser une liste des différents noeuds et messages impliqués dans le temps.

La seule propriété temporelle que nous avons testée est celle du blocage.

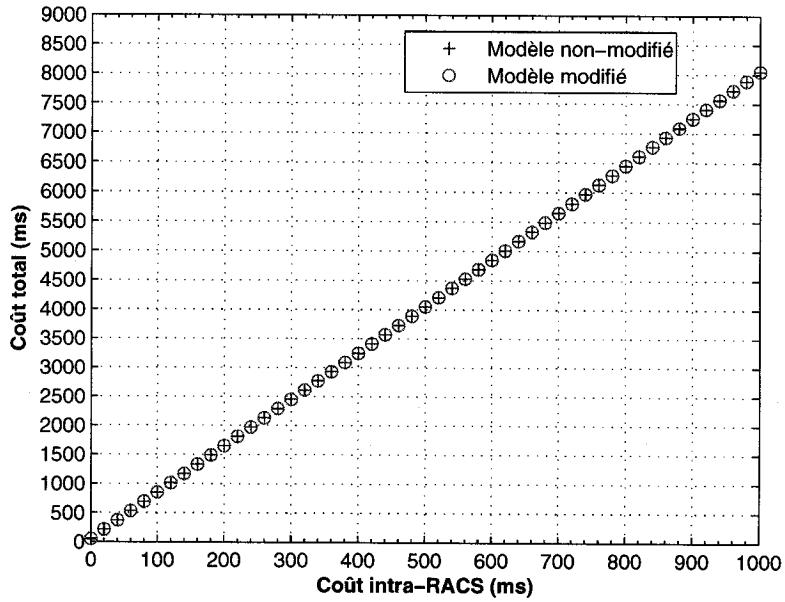

FIGURE 4.8 Coût total versus le $C_{INTRA-RACS}$ du scénario de réservation de ressources intra-domaine

La propriété de blocage (*A[] not deadlock*) permet de vérifier que le protocole ne bloquera jamais. Dans notre cas, la satisfaction de cette propriété nous est suffisante pour prouver que le processus est bien défini, car si l'une des étapes n'avait pas fonctionné, nous serions en blocage.

4.2.3 Réservation de ressources dans un réseau visité sans IMS avant les modifications

Dans cette sous-section, le processus original de réservation de ressources dans le réseau visité sans l'utilisation de l'IMS sera analysé. Ce sera fait à l'aide d'un modèle analytique et d'une validation formelle.

La Figure 4.9 montre le diagramme de séquence pour la réservation de ressources dans un réseau visité sans l'utilisation de l'IMS avant les modifications.

Nous en déduirons un modèle analytique qui permettra de comparer ses performances avec celles du modèle modifié. Nous utiliserons la liste des variables présentée au début du Volet 2.

Le processus sans modification engendre donc le modèle suivant :

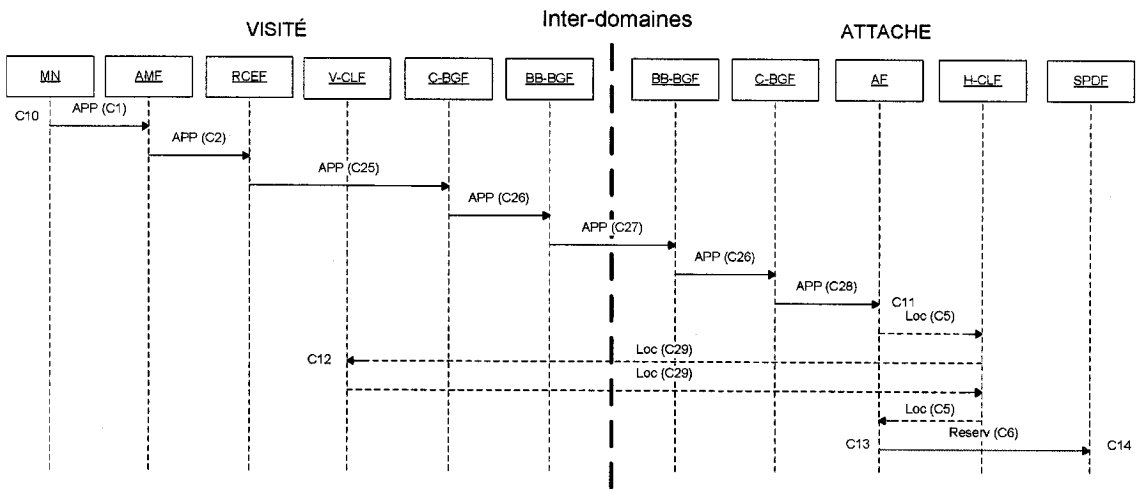

FIGURE 4.9 Scénario de réservation dans un réseau visité sans IMS avant les modifications

$$C_{10} + C_1 + C_2 + C_{25} + C_{26} + C_{27} + C_{26} + C_{28} + C_{11} + C_5 +$$
$$C_{29} + C_{12} + C_{29} + C_5 + C_{13} + C_6 + C_{14}$$

$$= C_1 + C_2 + 2 * C_5 + C_6 + C_{10} + C_{11} + C_{12} + C_{13} + C_{14} +$$
$$C_{25} + 2 * C_{26} + C_{27} + C_{28} + 2 * C_{29}$$

Il est important de noter que le processus est incomplet. En effet, le TISPAN n'a défini aucun processus pour traiter la requête de réservation dans le réseau d'attache et la transférer dans le réseau visité. C'est justement cette modification qui a été effectuée dans la prochaine sous-section. Nous nous servirons quand même de ce modèle comme borne inférieure pour la version modifiée.

Nous fixerons des coûts au modèle non-modifié et en ferons varier quelque-uns dans la section suivante dans le but de le comparer avec le modèle modifié.

Nous avons ensuite utilisé le logiciel UPPAAL pour effectuer la validation formelle du processus non-modifié, afin de vérifier que le processus proposé par le TISPAN était fonctionnel. Plus précisément, nous avons créé un fichier UPPAAL contenant une version originale du processus de réservation de ressources lorsque l'usager est dans un réseau visité. Ce fichier est disponible par le biais du groupe

LARIM de l'École Polytechnique de Montréal.

La version réalisée est une version qui correspond plus à une preuve de concept qu'à un modèle complet. En effet, dans ce modèle, il y a aucune gestion d'exception. Le but ultime de ce modèle est de vérifier que le processus peut fonctionner sans blocage, et par le fait même dresser une liste des différents noeuds et messages impliqués dans le temps.

La seule propriété temporelle que nous avons testée est celle du blocage.

La propriété de blocage (*A[] not deadlock*) nous permet de vérifier que le protocole ne bloquera jamais. Dans ce cas-ci, cette propriété n'est pas satisfaite, car le RACS du domaine d'attache ne sait pas comment traiter cette requête. Le processus n'est donc pas fonctionnel.

4.2.4 Réservation de ressources dans un réseau visité sans IMS après les modifications

Dans cette sous-section, le processus modifié de réservation de ressources dans un réseau visité sera analysé. Ce sera fait à l'aide d'un modèle analytique et d'une validation formelle.

La Figure 4.10 montre le diagramme de séquence pour la réservation de ressources dans un réseau d'attache sans IMS après les modifications.

Nous en déduirons un modèle analytique qui permettra de comparer ses performances avec celles du modèle non-modifié qui a été présenté à la section précédente. Nous utiliserons la liste des variables présentée au début du Volet 2.

Le processus avec modifications engendre donc le modèle suivant :

$$C_{10} + C_1 + C_2 + C_{25} + C_{26} + C_{27} + C_{26} + C_{28} + C_{11} +$$

$$C_{13} + C_{20} + C_{32} + C_{33} + C_{32} + C_{23} + C_{24} + C_{22} + C_{19} +$$

$$C_9 + C_{18} + C_{19} + C_{21} + C_{17} + C_9 + C_{21} + C_{16} + C_{22} +$$

$$C_{32} + C_{33} + C_{32} + C_{20} + C_{28} + C_{26} + C_{27} + C_{26} + C_{25} +$$

$$C_2 + C_1$$

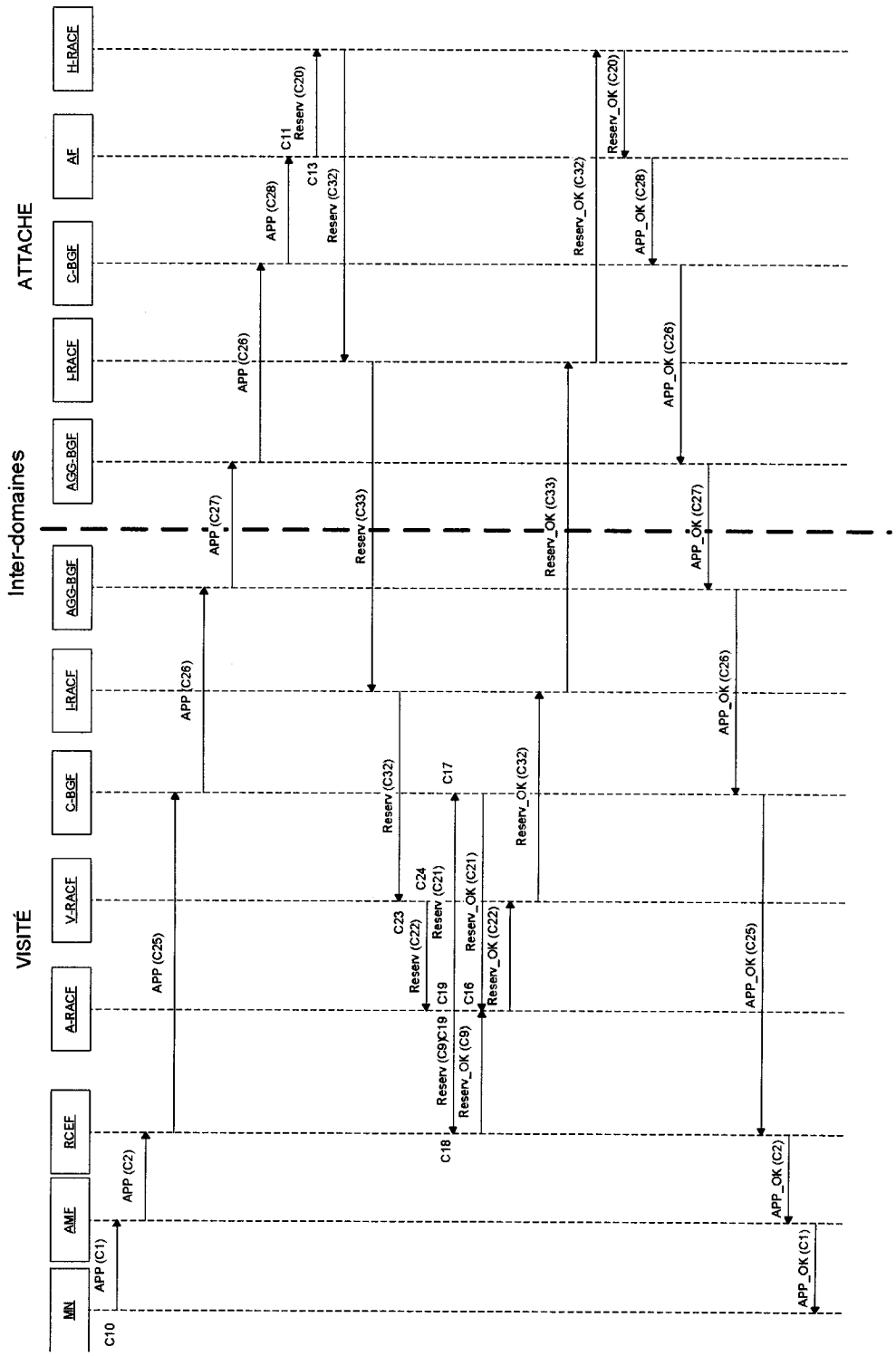

FIGURE 4.10 Scénario de réservation dans un réseau visité sans IMS après les modifications

$$= 2 * C_1 + 2 * C_2 + 2 * C_9 + C_{10} + C_{11} + C_{13} + C_{16} + C_{17} +$$

$$C_{18} + 2 * C_{19} + 2 * C_{20} + 2 * C_{21} + 2 * C_{22} + C_{23} + C_{24} +$$

$$2 * C_{25} + 4 * C_{26} + 2 * C_{27} + 2 * C_{28} + 4 * C_{32} + 2 * C_{33}$$

Nous faisons les hypothèses simplificatrices suivantes pour rendre plus facilement comparable les deux modèles (sans modification et avec modifications) :

- puisque la localisation est optionnelle, elle est enlevée du modèle ($C_5 = C_{12} = C_{29} = 0$) ;
- les temps de traitement ou de création des requêtes sont au maximum de 1 ms.

Comme dans la section précédente, nous supposons que les coûts de création de requête et de traitement ne dépassent pas 1 ms (réaliste avec les vitesses des processeurs actuels).

Nous effectuons aussi les simplifications de variables suivantes :

- $C_{ACCES} = C_1 + C_2 + C_{25}$;
- $C_{INTER-DOMAINES} = C_{27} = C_{33}$;
- $C_{INTRA-DOMAINE} = C_{26} = C_{28} = C_{32}$;
- $C_{INTRA-RACS} = C_6 = C_9 = C_{20} = C_{21} = C_{22}$.

Avec les simplifications et les hypothèses simplificatrices précédentes, le modèle sans modification devient :

$$C_{total-non-modifie} = C_{ACCES} + C_6 + 1ms + 1ms + 1ms + 1ms + 2 * C_{26} + C_{27} + C_{28}$$

$$C_{total-non-modifie} = C_{ACCES} + 2 * C_{INTRA-DOMAINE} + C_{INTER-DOMAINES} +$$

$$2 * C_{INTRA-RACS} + 4ms$$

Avec les même simplifications, le modèle modifié devient :

$$C_{total-modifie} = 2 * C_{ACCES} + 2 * C_{INTRA-RACS} + 1ms + 1ms + 1ms + 1ms + 1ms +$$

$$1ms + 2ms + 2 * C_{INTRA-RACS} + 2 * C_{INTRA-RACS} + 2 * C_{INTRA-RACS} + 1ms + 1ms +$$
$$4 * C_{INTRA-DOMAINE} + 2 * C_{INTER-DOMAINES} + 2 * C_{INTRA-DOMAINE} +$$
$$4 * C_{INTRA-DOMAINE} + 2 * C_{INTER-DOMAINES}$$

$$C_{total-modifie} = 2 * C_{ACCES} + 10 * C_{INTRA-DOMAINE} +$$
$$4 * C_{INTER-DOMAINES} + 8 * C_{INTRA-RACS} + 10ms$$

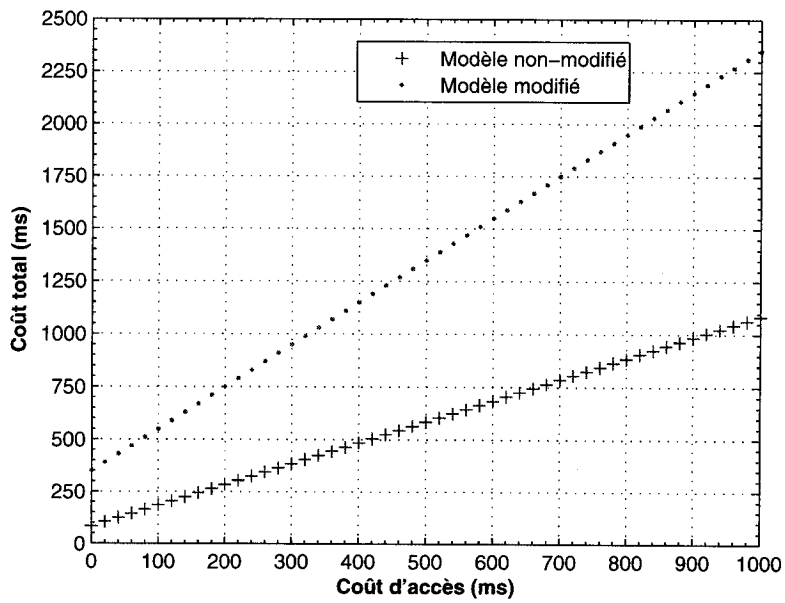

FIGURE 4.11 Coût total versus le C_{ACCES} pour la réservation inter-domaine sans IMS

Puisque les deux modèles se réduisent maintenant à 4 variables, nous allons faire 4 graphiques avec, dans chacun d'eux, trois variables fixes et une variable non-fixe. Cela revient à faire une étude de type *un facteur à la fois* et cela permet de déterminer l'importance de chacune des variables. Cependant, tous les cas ne seront pas explorés, comme le montrent les Figures 4.11 à 4.14.

Le premier graphique représente le coût total en temps versus C_{ACCES}. La liste suivante donne les variables fixées ainsi que leur valeur :

- $C_{INTRA-DOMAINE} = 10$ ms ;

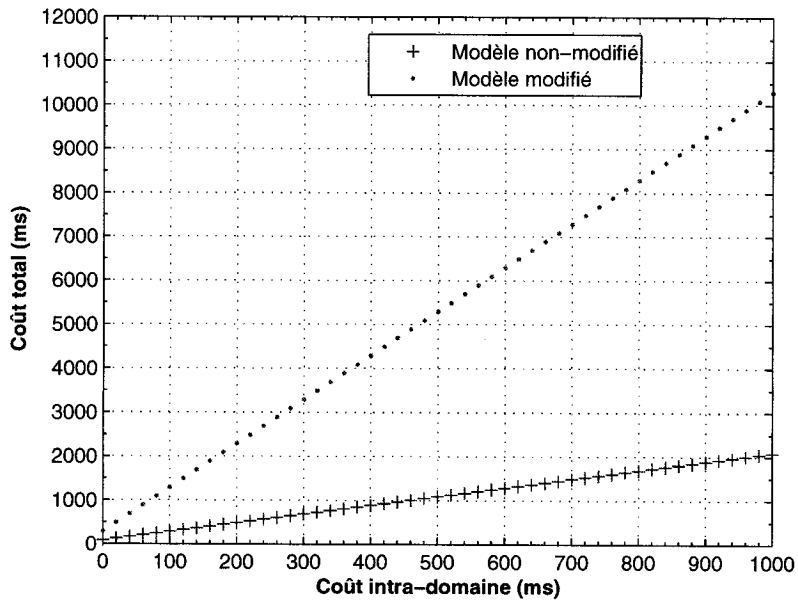

FIGURE 4.12 Coût total versus le $C_{INTRA-DOMAINE}$ pour la réservation inter-domaine sans IMS

- $C_{INTER-DOMAINES} = 50$ ms ;
- $C_{INTRA-RACS} = 5$ ms.

La Figure 4.11 montre le premier graphique. Nous y voyons bien l'effet du facteur 2 qui multiplie C_{ACCES} dans le modèle modifié versus le facteur 1 dans le modèle non-modifié. Cela équivaut à une croissance 2 fois plus grande.

Le second graphique représente le coût total en temps versus $C_{INTRA-DOMAINE}$. La liste suivante donne les variables fixées ainsi que leur valeur :

- $C_{ACCES} = 20$ ms ;
- $C_{INTER-DOMAINES} = 50$ ms ;
- $C_{INTRA-RACS} = 5$ ms.

La Figure 4.12 montre le deuxième graphique. Nous y voyons bien l'effet du facteur 10 qui multiplie $C_{INTRA-DOMAINE}$ dans le modèle modifié versus le facteur 2 dans le modèle non-modifié. Cela équivaut à une croissance 5 fois plus grande.

Le troisième graphique représente le coût total en temps versus $C_{INTER-DOMAINES}$. La liste suivante donne les variables fixées ainsi que leur valeur :

- $C_{INTRA-DOMAINE} = 10$ ms ;
- $C_{ACCES} = 20$ ms ;

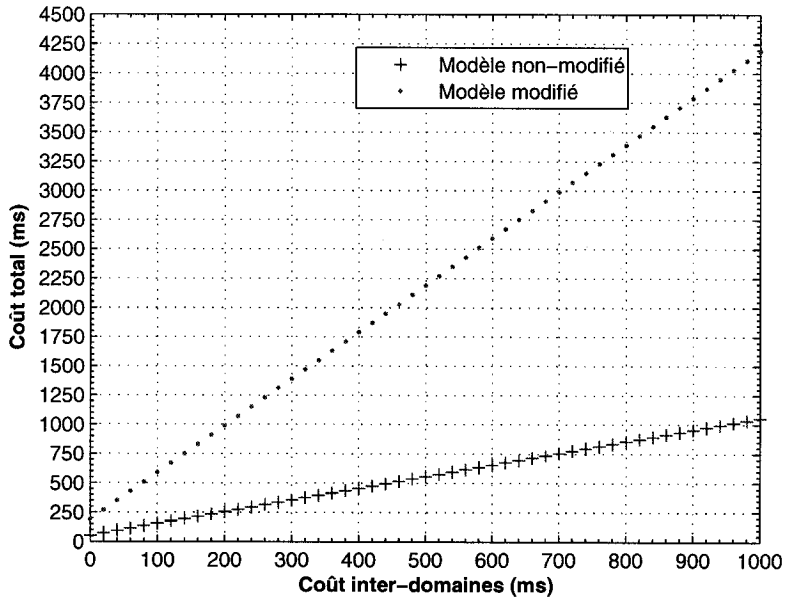

FIGURE 4.13 Coût total versus le $C_{INTER-DOMAINES}$ pour la réservation inter-domaine sans IMS

- $C_{INTRA-RACS} = 5$ ms.

La Figure 4.13 montre le troisième graphique. Nous y voyons bien l'effet du facteur 4 qui multiplie $C_{INTER-DOMAINES}$ dans le modèle modifié versus le facteur 1 dans le modèle non-modifié. Cela équivaut à une croissance 4 fois plus grande.

Le quatrième graphique représente le coût total en temps versus $C_{INTRA-RACS}$. La liste suivante donne les variables fixées ainsi que leur valeur :

- $C_{INTRA-DOMAINE} = 10$ ms ;
- $C_{INTER-DOMAINES} = 50$ ms ;
- $C_{ACCES} = 20$ ms.

La Figure 4.14 montre le quatrième graphique. Nous y voyons bien l'effet du facteur 8 qui multiplie $C_{INTRA-RACS}$ dans le modèle modifié versus le facteur 2 dans le modèle non-modifié. Cela équivaut à une croissance 4 fois plus grande.

Pour des valeurs normales de coûts ($C_{ACCES} = 20$ ms, $C_{INTRA-DOMAINE} = 10$ ms, $C_{INTER-DOMAINES} = 50$ ms et $C_{INTRA-RACS} = 5$ ms), on trouve un coût total de 104 ms pour le modèle non-modifié et de 390 ms pour le modèle modifié. Puisque le modèle non-modifié est incomplet, on ne peut pas se comparer avec cette valeur. Par contre, un délai de 390 ms est très acceptable lorsqu'un usager veut démarrer

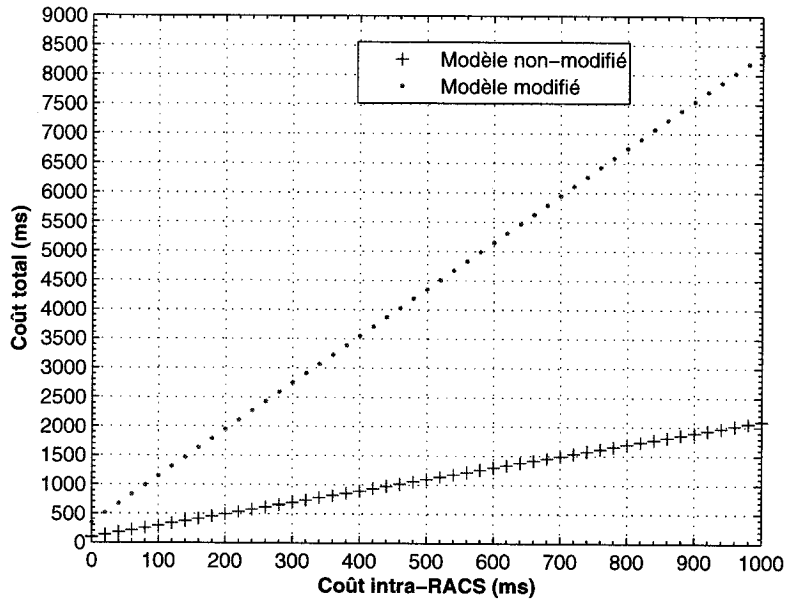

FIGURE 4.14 Coût total versus le $C_{INTRA-RACS}$ pour la réservation inter-domaine sans IMS

une nouvelle application qui nécessite une réservation de ressources.

Nous avons ensuite utilisé le logiciel UPPAAL pour effectuer la validation formelle du processus modifié. Plus précisément, nous avons créé un fichier UPPAAL contenant une version du processus modifié de réservation de ressources lorsque l'usager est dans un réseau visité sans IMS. Ce fichier est disponible par le biais du groupe LARIM de l'École Polytechnique de Montréal.

La version réalisée est une version qui correspond plus à une preuve de concept qu'à un modèle complet. En effet, dans ce modèle, il y a aucune gestion d'exception. Le but ultime de ce modèle est de vérifier que le processus peut fonctionner sans blocage, et par le fait même dresser une liste des différents noeuds et messages impliqués dans le temps.

La seule propriété temporelle que nous avons testée est celle du blocage.

La propriété de blocage (*A[] not deadlock*) nous permet de vérifier que le protocole ne bloquera jamais. Dans notre cas, la satisfaction de cette propriété nous est suffisante pour prouver que le processus est bien défini, car si l'une des étapes n'avait pas fonctionné, nous serions en blocage.

4.2.5 Réservation de ressources dans un réseau visité avec IMS avant les modifications

Dans cette sous-section, le processus original de réservation de ressources dans le réseau visité avec l'utilisation de l'IMS sera analysé. Ce sera fait à l'aide d'un modèle analytique et d'une validation formelle.

La Figure 4.15 montre le diagramme de séquence pour la réservation de ressources dans un réseau visité avant les modifications.

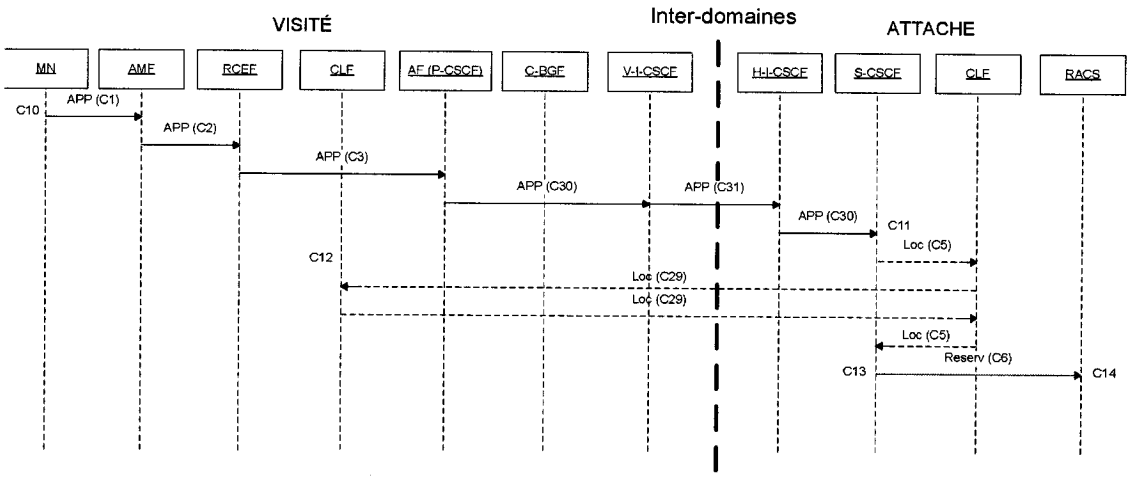

FIGURE 4.15 Scénario de réservation dans un réseau visité avec IMS avant les modifications

Nous en découlerons un modèle analytique qui permettra de comparer ses performances avec celles du modèle modifié. Nous utiliserons la liste des variables présentée au début du Volet 2.

Le processus sans modification engendre donc le modèle suivant :

$$C_{10} + C_1 + C_2 + C_3 + C_{30} + C_{31} + C_{30} + C_{11} + C_5 + C_{29} + C_{12} +$$
$$C_{29} + C_5 + C_{13} + C_6 + C_{14}$$

$$= C_1 + C_2 + C_3 + 2 * C_5 + C_6 + C_{10} + C_{11} + C_{12} + C_{13} + C_{14} +$$
$$2 * C_{29} + 2 * C_{30} + C_{31}$$

Il est important de noter que le processus est incomplet. En effet, le TISPAN

n'a défini aucun processus pour traiter la requête de réservation dans le réseau d'attache et la transférer dans le réseau visité. C'est justement cette modification qui sera effectuée dans la prochaine sous-section. Nous nous servirons quand même de ce modèle comme borne inférieure pour évaluer la version modifiée.

Nous fixerons des coûts au modèle non-modifié et en ferons varier quelque-uns dans la section suivante dans le but de le comparer avec le modèle modifié.

4.2.6 Réservation de ressources dans un réseau visité avec IMS après les modifications

Dans cette sous-section, le processus modifié de réservation de ressources dans un réseau visité avec l'utilisation d'IMS sera analysé. Ce sera fait à l'aide d'un modèle analytique et d'une validation formelle. Nous utiliserons la liste des variables présentée au début du Volet 2.

La Figure 4.16 montre le diagramme de séquence pour la réservation de ressources dans un réseau d'attache avec IMS après les modifications.

Le processus avec modifications engendre donc le modèle suivant :

$$C_{10} + C_1 + C_2 + C_3 + C_{30} + C_{31} + C_{30} + C_{11} +$$

$$C_{13} + C_6 + C_{32} + C_{33} + C_{32} + C_{23} + C_{24} + C_{22} +$$

$$C_{19} + C_9 + C_{18} + C_{19} + C_{21} + C_{17} + C_9 + C_{21} +$$

$$C_{16} + C_{22} + C_{32} + C_{20} + C_3 + C_{33} + C_2 + C_{32} + C_1$$

$$= 2 * C_1 + 2 * C_2 + 2 * C_3 + C_6 + 2 * C_9 + C_{10} + C_{11} +$$

$$C_{13} + C_{16} + C_{17} + C_{18} + 2 * C_{19} + C_{20} + 2 * C_{21} +$$

$$2 * C_{22} + C_{23} + C_{24} + 2 * C_{30} + C_{31} + 4 * C_{32} + 2 * C_{33}$$

Nous faisons les hypothèses simplificatrices suivantes pour rendre plus facilement comparable les deux modèles (sans modification et avec modifications) :

- puisque la localisation est optionnelle, elle est enlevée du modèle ($C_5 = C_{12} = C_{29} = 0$) ;
- les temps de traitement ou de création des requêtes sont d'au maximum 1 ms.

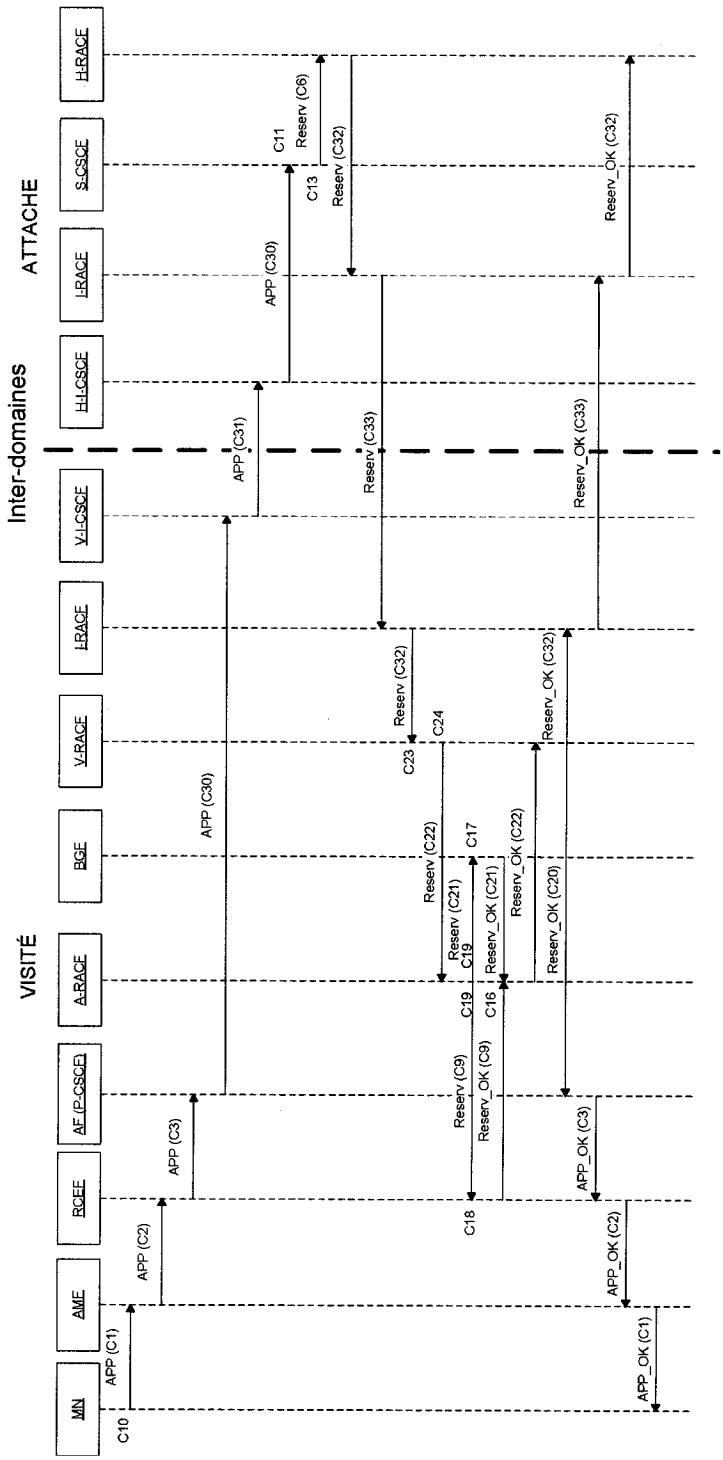

FIGURE 4.16 Scénario de réservation dans un réseau visité avec IMS après les modifications

Comme dans la section précédente, nous supposons que les coûts de création de requête et de traitement ne dépassent pas 1 ms (réaliste avec les vitesses des processeurs actuels).

Nous effectuons aussi les simplifications de variables suivantes :

- $C_{ACCES} = C_1 + C_2 + C_3$;
- $C_{INTER-DOMAINES} = C_{31} = C_{33}$;
- $C_{INTRA-DOMAINE} = C_{30} = C_{32}$;
- $C_{INTRA-RACS} = C_6 = C_9 = C_{20} = C_{21} = C_{22}$.

Avec les simplifications et les hypothèses simplificatrices précédentes le modèle sans modification devient :

$$C_{total-non-modifie} = C_{ACCES} + C_{INTRA-RACS} + 1ms + 1ms + 1ms + 1ms + 1ms +$$

$$2 * C_{INTRA-DOMAINE} + C_{INTER-DOMAINES}$$

$$C_{total-non-modifie} = C_{ACCES} + 2 * C_{INTRA-DOMAINE} + C_{INTER-DOMAINES} +$$

$$C_{INTRA-RACS} + 5ms$$

Avec les mêmes simplifications, le modèle modifié devient :

$$C_{total-modifie} = 2 * C_{ACCES} + C_{INTRA-RACS} + 2 * C_{INTRA-RACS} + 1ms + 1ms +$$

$$1ms+1ms+1ms+1ms+2ms+5*C_{INTRA-RACS}+1ms+1ms+2*C_{INTRA-DOMAINE}$$

$$+C_{INTER-DOMAINES} + 4 * C_{INTRA-DOMAINE} + 2 * C_{INTER-DOMAINES}$$

$$C_{total-modifie} = 2 * C_{ACCES} + 6 * C_{INTRA-DOMAINE} +$$

$$3 * C_{INTER-DOMAINES} + 8 * C_{INTRA-RACS} + 10ms$$

Puisque les deux modèles se réduisent maintenant à 4 variables, nous allons faire 4 graphiques avec dans chacun d'eux trois variables fixes et une variable non-

fixe. Cela revient à faire une étude de type *un facteur à la fois* et cela permet de déterminer l'importance de chacune des variables. Cependant, tous les cas ne seront pas explorés, comme le montrent les Figures 4.17 à 4.20.

Le premier graphique représente le coût total en temps versus C_{ACCES}. La liste suivante donne les variables fixées ainsi que leur valeur :

- $C_{INTRA-DOMAINE} = 10$ ms ;
- $C_{INTER-DOMAINES} = 50$ ms ;
- $C_{INTRA-RACS} = 5$ ms.

La Figure 4.17 montre le premier graphique. Nous y voyons bien l'effet du facteur 2 qui multiplie C_{ACCES} dans le modèle modifié versus le facteur 1 dans le modèle non-modifié. Cela équivaut à une croissance 2 fois plus grande.

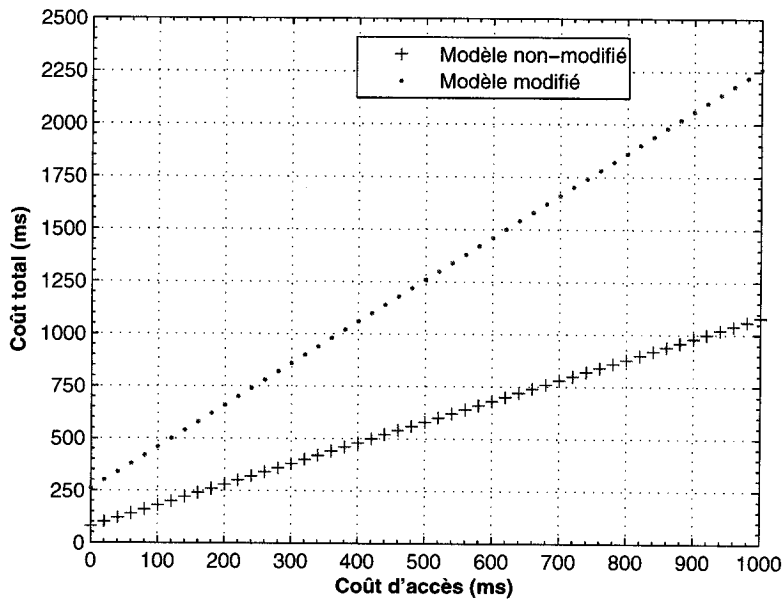

FIGURE 4.17 Coût total versus le C_{ACCES} pour la réservation inter-domaine avec IMS

Le second graphique représente le coût total en temps versus $C_{INTRA-DOMAINE}$. La liste suivante donne les variables fixées ainsi que leur valeur :

- $C_{ACCES} = 20$ ms ;
- $C_{INTER-DOMAINES} = 50$ ms ;
- $C_{INTRA-RACS} = 5$ ms.

La Figure 4.18 montre le deuxième graphique. Nous y voyons bien l'effet du facteur 6 qui multiplie $C_{INTRA-DOMAINE}$ dans le modèle modifié versus le facteur 2 dans le modèle non-modifié. Cela équivaut à une croissance 3 fois plus grande.

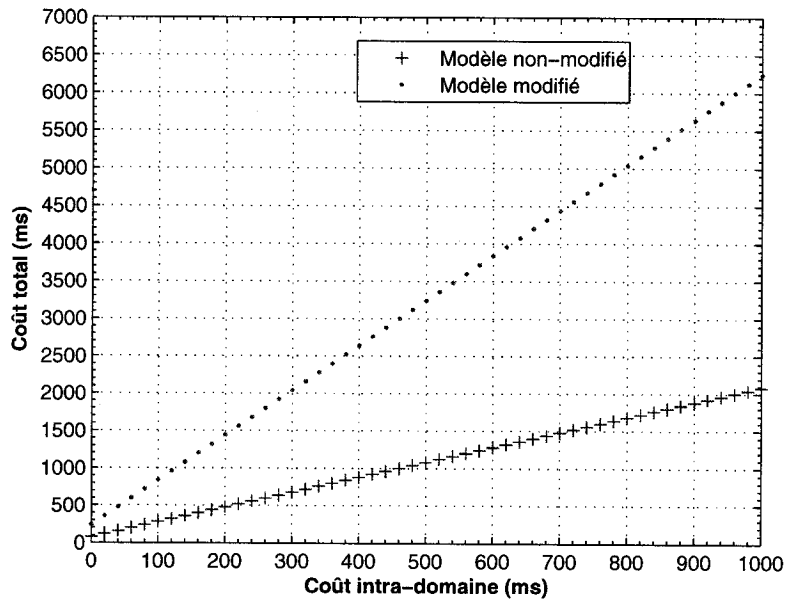

FIGURE 4.18 Coût total versus le $C_{INTRA-DOMAINE}$ pour la réservation inter-domaine avec IMS

Le troisième graphique représente le coût total en temps versus $C_{INTER-DOMAINES}$. La liste suivante donne les variables fixées ainsi que leur valeur :

- $C_{INTRA-DOMAINE} = 10$ ms ;
- $C_{ACCES} = 20$ ms ;
- $C_{INTRA-RACS} = 5$ ms.

La Figure 4.19 montre le troisième graphique. Nous y voyons bien l'effet du facteur 3 qui multiplie $C_{INTER-DOMAINES}$ dans le modèle modifié versus le facteur 1 dans le modèle non-modifié. Cela équivaut à une croissance 3 fois plus grande.

Le quatrième graphique représente le coût total en temps versus $C_{INTRA-RACS}$. La liste suivante donne les variables fixées ainsi que leur valeur :

- $C_{INTRA-DOMAINE} = 10$ ms ;
- $C_{INTER-DOMAINES} = 50$ ms ;
- $C_{ACCES} = 20$ ms.

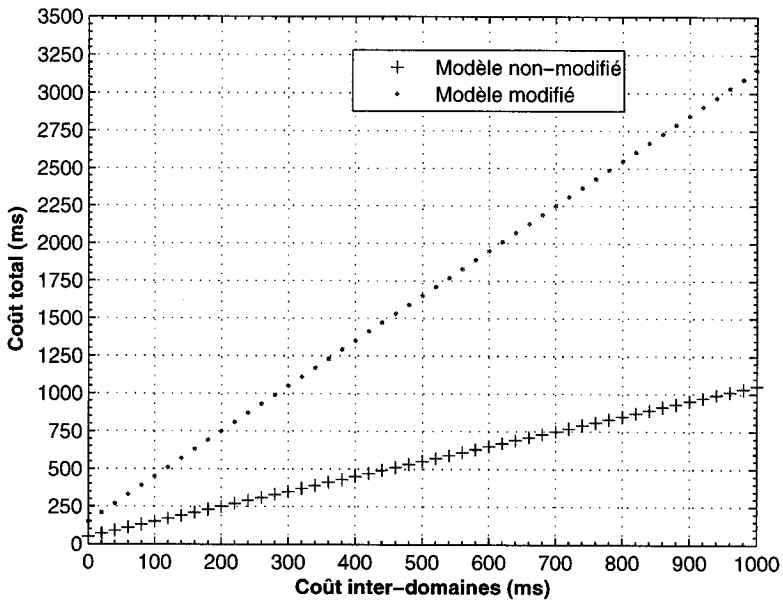

FIGURE 4.19 Coût total versus le $C_{INTER-DOMAINES}$ pour la réservation inter-domaine avec IMS

La Figure 4.20 montre le quatrième graphique. Nous y voyons bien l'effet du facteur 8 qui multiplie $C_{INTRA-RACS}$ dans le modèle modifié versus le facteur 1 dans le modèle non-modifié. Cela équivaut à une croissance 8 fois plus grande.

Pour des valeurs normales de coûts (C_{ACCES} = 20 ms, $C_{INTRA-DOMAINE}$ = 10 ms, $C_{INTER-DOMAINES}$ = 50 ms et $C_{INTRA-RACS}$ = 5 ms), on trouve un coût total de 100 ms pour le modèle non-modifié et de 300 ms pour le modèle modifié. Puisque le modèle non-modifié est incomplet, on ne peut pas se comparer avec cette valeur. Par contre, un délai de 300 ms est très acceptable lorsqu'un usager veut démarrer une nouvelle application qui nécessite une réservation de ressources. De plus, le délai est inférieur au délai sans IMS de 90ms (sans IMS= 390 ms).

Nous avons ensuite utilisé le logiciel UPPAAL pour effectuer la validation formelle du processus modifié. Plus précisément, nous avons créé un fichier UPPAAL contenant une version du processus modifié de réservation de ressources lorsque l'usager est dans un réseau visité avec IMS. Ce fichier est disponible par le biais du groupe LARIM de l'École Polytechnique de Montréal.

La version réalisée est une version qui correspond plus à une preuve de concept qu'à un modèle complet. En effet, dans ce modèle, il n'y a aucune gestion d'excep-

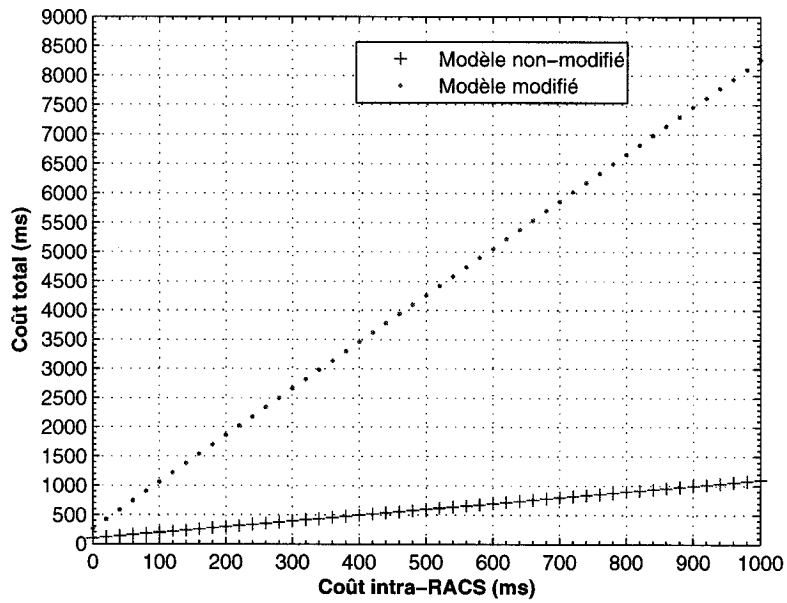

FIGURE 4.20 Coût total versus le $C_{INTRA-RACS}$ pour la réservation inter-domaine avec IMS

tion. Le but ultime de ce modèle est de vérifier que le processus peut fonctionner sans blocage, et par le fait même dresser une liste des différents noeuds et messages impliqués dans le temps.

La seule propriété temporelle que nous avons testée est celle du blocage.

La propriété de blocage (*A[] not deadlock*) nous permet de vérifier que le protocole ne bloquera jamais. Dans notre cas, la satisfaction de cette propriété nous est suffisante pour prouver que le processus est bien défini, car si l'une des étapes n'avait pas fonctionné, nous serions en blocage.

4.2.7 Réservation de ressources dans un réseau visité avec le serveur d'applications dans le réseau visité avant les modifications

Le TISPAN n'a prévu aucun mécanisme pour gérer une telle situation, donc aucun modèle analytique ou validation formelle ne sera fait dans cette section. Un mécanisme pour gérer ce scénario est présenté à la prochaine sous-section.

4.2.8 Réservation de ressources dans un réseau visité avec le serveur d'applications dans le réseau visité après les modifications

Dans cette sous-section, le nouveau processus de réservation de ressources dans un réseau visité avec le serveur d'application dans le même domaine sera analysé. Ce sera fait à l'aide d'un modèle analytique et d'une validation formelle. Nous utiliserons la liste des variables présentée au début du Volet 2.

La Figure 4.21 montre le diagramme de séquence pour la réservation de ressources dans un réseau visité avec le serveur d'applications dans le même réseau.

Le processus engendre donc le modèle suivant :

$$C_{10} + C_1 + C_2 + C_3 + C_{11} + C_{13} + C_{20} + C_{23} +$$

$$C_{24} + C_{22} + C_{19} + C_9 + C_{18} + C_{19} + C_{21} + C_{17} +$$

$$C_9 + C_{21} + C_{16} + C_{22} + C_{34} + C_{20} + C_3 + C_2 + C_1 +$$

$$C_{32} + C_{33} + C_{32} + C_{35} + C_{32} + C_{33} + C_{32}$$

$$= 2 * C_1 + 2 * C_2 + 2 * C_3 + 2 * C_9 + C_{10} + C_{11} + C_{13} + C_{16} +$$

$$C_{17} + C_{18} + 2 * C_{19} + 2 * C_{20} + 2 * C_{21} + 2 * C_{22} + C_{23} +$$

$$C_{24} + 4 * C_{32} + 2 * C_{33} + C_{34} + C_{35}$$

Nous faisons l'hypothèse simplificatrice suivante pour rendre plus facilement analysable le modèle :

- les temps de traitement ou de création des requêtes sont au maximum de 1 ms.

Comme dans la section précédente, nous supposons que les coûts de création de requête et de traitement ne dépassent pas 1 ms (réaliste avec les vitesses des processeurs actuels).

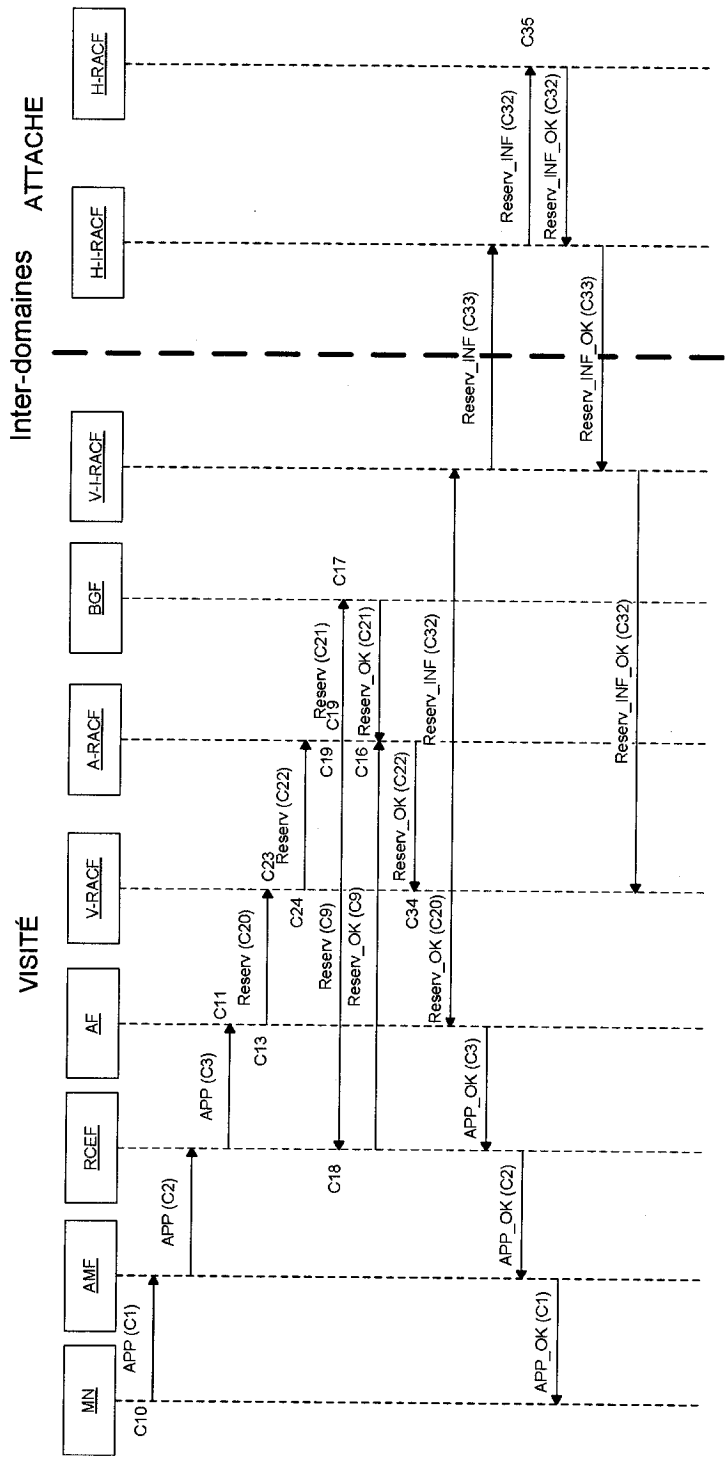

FIGURE 4.21 Scénario de réservation dans un réseau visité avec le serveur d'applications dans le réseau visité

Nous avons aussi effectué les simplifications de variables suivantes :

- $C_{ACCES} = C_1 + C_2 + C_3$;
- $C_{INTER-DOMAINES} = C_{33}$;
- $C_{INTRA-DOMAINE} = C_{32}$;
- $C_{INTRA-RACS} = C_6 = C_9 = C_{20} = C_{21} = C_{22}$.

Avec les simplifications et les hypothèses simplificatrices précédentes le modèle devient :

$$C_{total} = 2 * C_{ACCES} + 2 * C_{INTRA-RACS} + 1ms + 1ms + 1ms + 1ms + 1ms + 1ms +$$
$$2ms + 2 * C_{INTRA-RACS} + 2 * C_{INTRA-RACS} + 2 * C_{INTRA-RACS} + 1ms +$$
$$1ms + 4 * C_{INTRA-DOMAINE} + 2 * C_{INTER-DOMAINES} + 1ms + 1ms$$

$$C_{total} = 2 * C_{ACCES} + 4 * C_{INTRA-DOMAINE} + 2 * C_{INTER-DOMAINES} +$$
$$8 * C_{INTRA-RACS} + 12ms$$

Puisque le modèle se réduit maintenant à 4 variables, nous allons faire 4 graphiques avec trois variables fixes et une variable non-fixe dans chacun d'eux. Cela revient à faire une étude de type *un facteur à la fois* et cela permet de déterminer également l'importance de chacune des variables. Cependant, tous les cas ne seront pas explorés, comme le montrent les Figures 4.22 à 4.25.

Le premier graphique représente le coût total en temps versus C_{ACCES}. La liste suivante donne les variables fixées ainsi que leur valeur :

- $C_{INTRA-DOMAINE} = 10$ ms ;
- $C_{INTER-DOMAINES} = 50$ ms ;
- $C_{INTRA-RACS} = 5$ ms.

La Figure 4.22 montre le premier graphique. Nous y voyons bien l'effet du facteur 2 qui multiplie C_{ACCES} dans le modèle.

Le second graphique représente le coût total en temps versus $C_{INTRA-DOMAINE}$. La liste suivante donne les variables fixées ainsi que leur valeur :

- $C_{ACCES} = 20$ ms ;

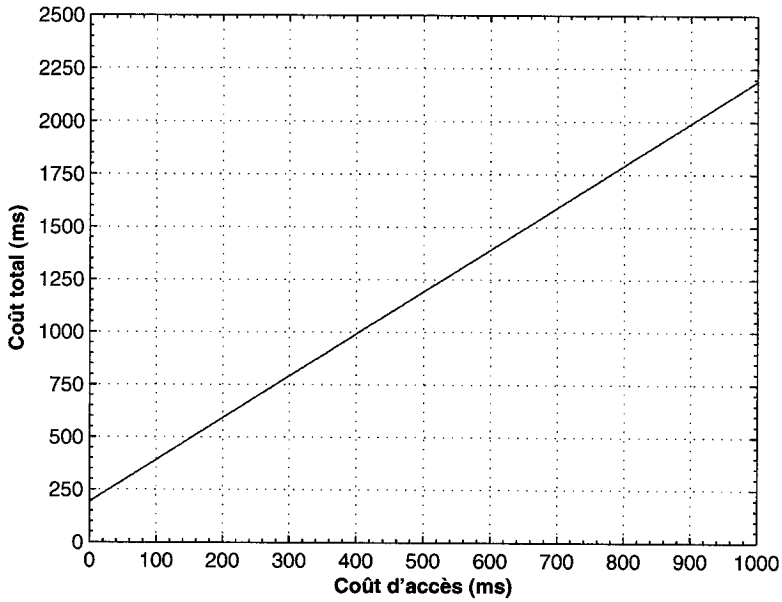

FIGURE 4.22 Coût total versus le C_{ACCES} pour la réservation inter-domaines avec le serveur d'applications dans le réseau visité

- $C_{INTER-DOMAINES} = 50$ ms ;
- $C_{INTRA-RACS} = 5$ ms.

La Figure 4.23 montre le deuxième graphique. Nous y voyons bien l'effet du facteur 4 qui multiplie $C_{INTRA-DOMAINE}$ dans le modèle.

Le troisième graphique représente le coût total en temps versus $C_{INTER-DOMAINES}$. La liste suivante donne les variables fixées ainsi que leur valeur :

- $C_{INTRA-DOMAINE} = 10$ ms ;
- $C_{ACCES} = 20$ ms ;
- $C_{INTRA-RACS} = 5$ ms.

La Figure 4.24 montre le troisième graphique. Nous y voyons bien l'effet du facteur 2 qui multiplie $C_{INTER-DOMAINES}$ dans le modèle.

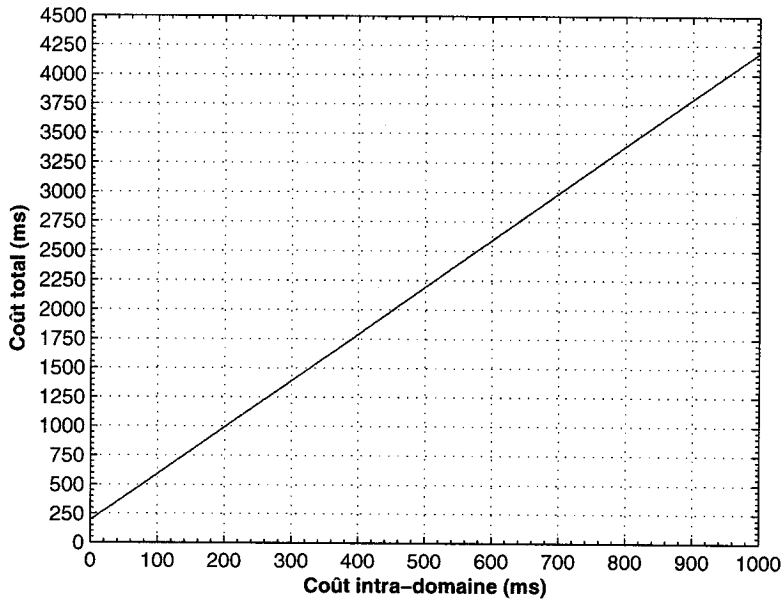

FIGURE 4.23 Coût total versus le $C_{INTRA-DOMAINE}$ pour la réservation inter-domaines avec le serveur d'applications dans le réseau visité

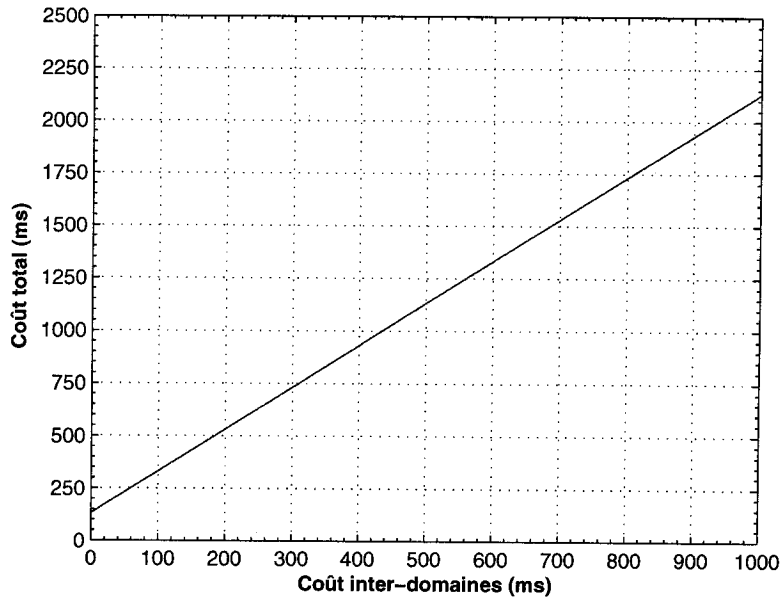

FIGURE 4.24 Coût total versus le $C_{INTER-DOMAINES}$ pour la réservation inter-domaines avec le serveur d'applications dans le réseau visité

Le quatrième graphique représente le coût total en temps versus $C_{INTRA-RACS}$. La liste suivante donne les variables fixées ainsi que leur valeur :

- $C_{INTRA-DOMAINE}$ = 10 ms ;
- $C_{INTER-DOMAINES}$ = 50 ms ;
- C_{ACCES} = 20 ms.

La Figure 4.25 montre le quatrième graphique. Nous y voyons bien l'effet du facteur 8 qui multiplie $C_{INTRA-RACS}$ dans le modèle.

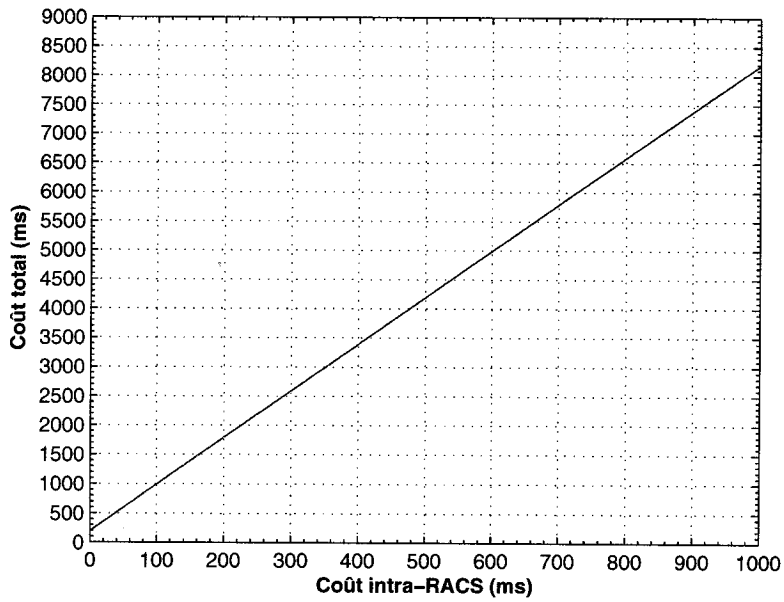

FIGURE 4.25 Coût total versus le $C_{INTRA-RACS}$ pour la réservation inter-domaines avec le serveur d'applications dans le réseau visité

Pour des valeurs normales de coûts (C_{ACCES} = 20 ms, $C_{INTRA-DOMAINE}$ = 10 ms, $C_{INTER-DOMAINES}$ = 50 ms et $C_{INTRA-RACS}$ = 5 ms), on trouve un coût total de 232 ms pour le modèle. Un délai de 232 ms est très acceptable lorsqu'un usager veut démarrer une nouvelle application qui nécessite une réservation de ressources. Ce délai est de 68 ms plus court que le scénario avec IMS et 158 ms plus court que le scénario sans IMS.

Nous avons ensuite utilisé le logiciel UPPAAL pour effectuer la validation formelle du processus. Plus précisément, nous avons créé un fichier UPPAAL contenant une version du processus de réservation de ressources lorsque l'usager est dans un

réseau visité avec le serveur d'applications dans le réseau visité.

La version réalisée est une version qui correspond plus à une preuve de concept qu'à un modèle complet. En effet, dans ce modèle, il n'y a aucune gestion d'exception. Le but ultime de ce modèle est de vérifier que le processus peut fonctionner sans blocage, et par le fait même dresser une liste des différents noeuds et messages impliqués dans le temps.

La seule propriété temporelle que nous avons testée est celle du blocage.

La propriété de blocage (*A[] not deadlock*) nous permet de vérifier que le protocole ne bloquera jamais. Dans notre cas, la satisfaction de cette propriété nous est suffisante pour prouver que le processus est bien défini, car si l'une des étapes n'avait pas fonctionné, nous serions en blocage.

4.2.9 Modèle combiné

Dans cette section, nous allons comparer les délais moyens des 4 scénarios. Nous allons aussi tracer le graphique résultant de la combinaison des 4 modèles.

Le Tableau 4.4 montre les délais de chacun des scénarios originaux et de ceux modifiés. Voici le nom de chacun des scénario :

1. l'usager est dans son réseau d'attache ;
2. l'usager est dans un réseau visité sans l'utilisation d'IMS ;
3. l'usager est dans un réseau visité avec l'utilisation d'IMS ;
4. l'usager est dans un réseau visité et utilise le serveur d'applications du réseau visité.

Il est intéressant de noter qu'il y a une réduction considérable des délais entre l'utilisation du serveur d'applications dans le réseau visité (scénario 4) et l'utilisation du serveur d'applications dans le réseau d'attache sans utiliser IMS (scénario 2). La différence est de 158 ms (390 ms-232 ms). Cependant, le scénario 4 ne peut pas être souvent utilisé puisque une mobilité complète des applications est rare et difficile à gérer. En effet, l'utilisation de ce type de serveurs d'applications (complètement dans le réseau visité) sera probablement utilisée pour les services de localisation et pour quelques autres rares services.

Nous fixons ensuite des probabilités pour chacun des scénarios afin de tracer un graphique cumulatif. Voici les probabilités que nous allons utiliser :

- scénario 1 : 0,70 ;

TABLEAU 4.4 Comparaison des délais moyen des 4 scénarios

Scénario	Délai moyen original	Délai moyen modifié
1	90 ms	90 ms
2	104 ms	390 ms
3	100 ms	300 ms
4	-	232 ms

- scénario 2 : 0,10 ;
- scénario 3 : 0,15 ;
- scénario 4 : 0,05.

Nous avons attribué une forte probabilité que l'usager soit dans son réseau d'attache, car nous croyons que c'est le principal patron d'utilisation des réseaux cellulaires. Ensuite, nous avons attribué une plus forte probabilité à l'utilisation d'IMS dans le réseau visité qu'à sa non-utilisation, car cette pratique devient rapidement la norme. Pour terminer, nous avons attribué une faible probabilité d'utiliser le serveur d'applications directement dans le réseau visité, car ce type de scénario est assez rare.

Il est important de noter que nous avons remplacé l'équation originale du scénario 4 par celle du scénario 3, puisqu'elle n'existe pas.

Voici les deux modèles résultants :

original :

$$0,70 * (2 * C_{ACCES} + 8 * C_{INTRA-RACS} + 10ms)+$$

$$0,10*(C_{ACCES}+2*C_{INTRA-DOMAINE}+C_{INTER-DOMAINES}+2*C_{INTRA-RACS}+4ms)+$$

$$0,15*(C_{ACCES}+2*C_{INTRA-DOMAINE}+C_{INTER-DOMAINES}+C_{INTRA-RACS}+5ms)+$$

$$0,05*(C_{ACCES}+2*C_{INTRA-DOMAINE}+C_{INTER-DOMAINES}+C_{INTRA-RACS}+5ms)$$

modifié :

$$0,70 * (2 * C_{ACCES} + 8 * C_{INTRA-RACS} + 10ms)+$$

$$0,10 * (2 * C_{ACCES} + 10 * C_{INTRA-DOMAINE} + 4 * C_{INTER-DOMAINES}+$$

$$8 * C_{INTRA-RACS} + 10ms)+$$

$$0,15 * (2 * C_{ACCES} + 6 * C_{INTRA-DOMAINE} + 3 * C_{INTER-DOMAINES} +$$
$$8 * C_{INTRA-RACS} + 10ms) +$$
$$0,05 * (2 * C_{ACCES} + 4 * C_{INTRA-DOMAINE} + 2 * C_{INTER-DOMAINES} +$$
$$8 * C_{INTRA-RACS} + 12ms)$$

Puisque les modèles comportent 4 variables, nous allons faire 4 graphiques avec trois variables fixes et une variable non-fixe dans chacun d'eux. Cela revient à faire une étude de type *un facteur à la fois* et cela permet de déterminer l'importance de chacune des variables. Cependant, tous les cas ne seront pas explorés. Dans les prochains paragraphes, vous retrouverez les 4 graphiques.

Le premier graphique représente le coût total en temps versus C_{ACCES}. La liste suivante donne les variables fixées ainsi que leur valeur :

- $C_{INTRA-DOMAINE} = 10$ ms ;
- $C_{INTER-DOMAINES} = 50$ ms ;
- $C_{INTRA-RACS} = 5$ ms.

La Figure 4.26 montre le premier graphique. Les deux courbes sont assez semblables puisque dans le modèle original un facteur 1,7 $(2*0,70+1*0,10+1*0,15+1*0,05)$ multiplie C_{ACCES} et un facteur 2 $(2*0,70+2*0,10+2*0,15+2*0,05)$ dans le modèle modifié.

Le second graphique représente le coût total en temps versus $C_{INTRA-DOMAINE}$. La liste suivante donne les variables fixées ainsi que leur valeur :

- $C_{ACCES} = 20$ ms ;
- $C_{INTER-DOMAINES} = 50$ ms ;
- $C_{INTRA-RACS} = 5$ ms.

La Figure 4.27 montre le deuxième graphique. Nous y voyons bien l'effet du facteur 2,1 $(0*0,70+10*0,10+6*0,15+4*0,05)$ qui multiplie $C_{INTRA-DOMAINE}$ dans le modèle modifié versus le facteur 0,6 $(0*0,70+2*0,10+2*0,15+2*0,05)$ dans le modèle original. Cette différence s'explique principalement par le fait que les modèles originaux applicables lorsque l'usager est dans son réseau visité sont incomplets, et donc en mode blocage. De plus, l'ajout de certaines fonctionnalités entraîne une augmentation de ce facteur.

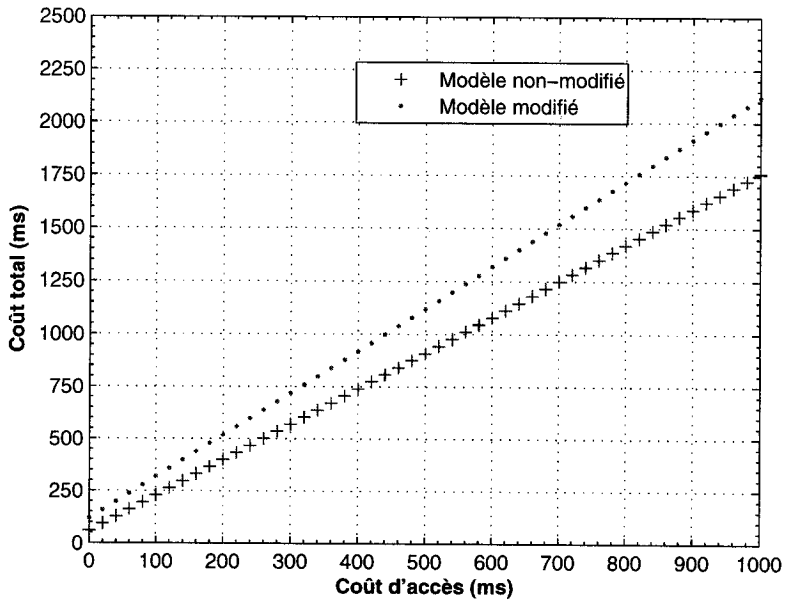

FIGURE 4.26 Coût total versus le C_{ACCES} pour le modèle combiné de réservation de ressources

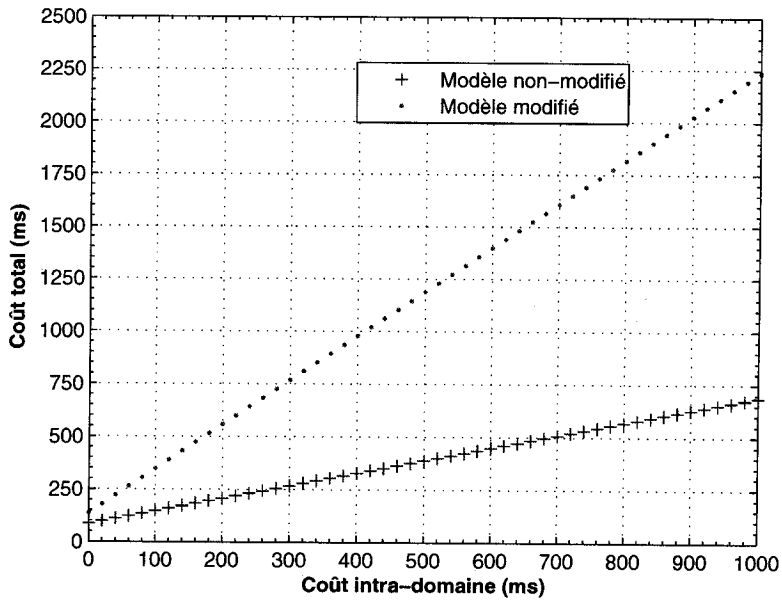

FIGURE 4.27 Coût total versus le $C_{INTRA-DOMAINE}$ pour le modèle combiné de réservation de ressources

Le troisième graphique représente le coût total en temps versus $C_{INTER-DOMAINES}$. La liste suivante donne les variables fixées ainsi que leur valeur :

- $C_{INTRA-DOMAINE} = 10$ ms ;
- $C_{ACCES} = 20$ ms ;
- $C_{INTRA-RACS} = 5$ ms.

La Figure 4.28 montre le troisième graphique. Nous y voyons bien l'effet du facteur 0,95 $(0*0,70+4*0,10+3*0,15+2*0,05)$ qui multiplie $C_{INTER-DOMAINES}$ dans le modèle modifié versus le facteur 0,30 $(0*0,70+1*0,10+1*0,15+1*0,05)$ dans le modèle original. Encore une fois, cette différence est due au fait que les modèles originaux sont incomplets.

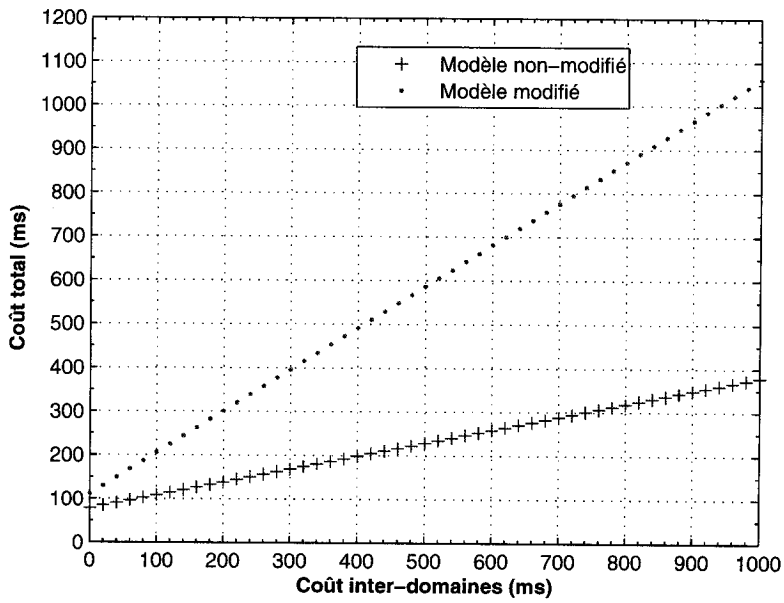

FIGURE 4.28 Coût total versus le $C_{INTER-DOMAINES}$ pour le modèle combiné de réservation de ressources

Le quatrième graphique représente le coût total en temps versus $C_{INTRA-RACS}$. La liste suivante donne les variables fixées ainsi que leur valeur :

- $C_{INTRA-DOMAINE} = 10$ ms ;
- $C_{INTER-DOMAINES} = 50$ ms ;
- $C_{ACCES} = 20$ ms.

La Figure 4.29 montre le quatrième graphique. Nous y voyons deux courbes semblables à cause du facteur 8 $(8*0,70+8*0,10+8*0,15+8*0,05)$ qui multiplie

$C_{INTRA-RACS}$ dans le modèle modifié versus le facteur 6 $(8 * 0,70 + 2 * 0,10 + 1 * 0,15 + 1 * 0,05)$ dans le modèle original. En effet, ces deux facteurs sont assez semblables.

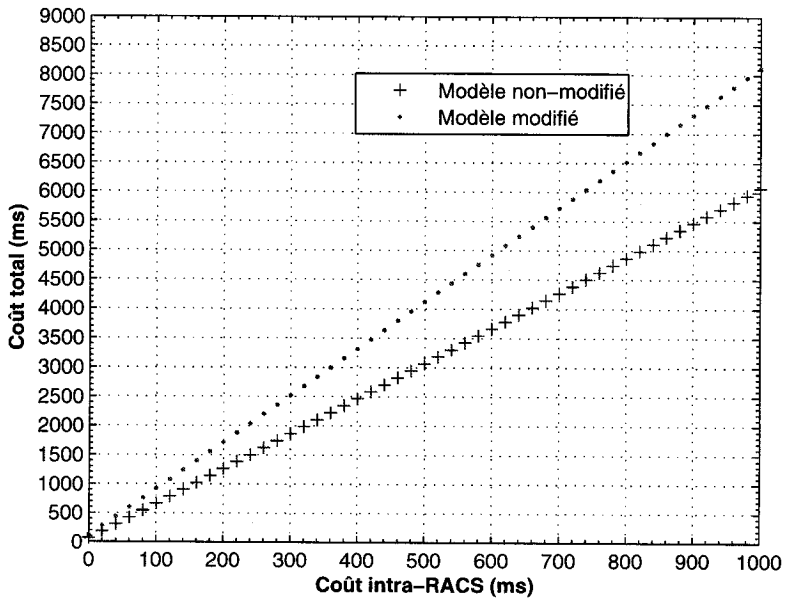

FIGURE 4.29 Coût total versus le $C_{INTRA-RACS}$ pour le modèle combiné de réservation de ressources

Pour des valeurs normales de coûts (C_{ACCES} = 20 ms, $C_{INTRA-DOMAINE}$ = 10 ms, $C_{INTER-DOMAINES}$ = 50 ms et $C_{INTRA-RACS}$ = 5 ms), on trouve un coût total de 93,4 ms pour le modèle original et 158,6 ms pour le modèle modifié. Un délai de 158,6 ms est très acceptable lorsqu'un usager veut démarrer une nouvelle application qui nécessite une réservation de ressources. La différence de 65,2 ms s'explique facilement par le fait que certains modèles originaux sont incomplets. Il est aussi important de noter qu'aucun usager ne sera capable de faire la différence au niveau des délais, mais il serait souhaitable qu'il n'en soit pas de même pour les nombreuses nouvelles fonctionnalités auxquelles il aura accès.

4.2.10 Mise à jour des réservations avant les modifications

Le TISPAN n'a prévu aucun mécanisme pour gérer une telle situation, donc aucun modèle analytique ou validation formelle ne sera fait dans cette section. Un

mécanisme pour gérer ce scénario est présenté à la prochaine sous-section.

4.2.11 Mise à jour des réservations après les modifications

Dans cette sous-section, le nouveau processus de mise à jour des réservations sera analysé. Ce sera fait à l'aide d'un modèle analytique.

Pour l'élaboration du modèle analytique de cette sous-section, nous allons utiliser des coûts différents puisque ce scénario est assez différent des autres modèles de ce volet. Voici donc la liste des coûts utilisés :

$C_{PDBF_{UPDATE}}$	C_1	Coût de la création du message d'avertissement de mise à jour du PDBF.
$C_{RACF_{LOCAL-RULES}}$	C_5	Coût de la création du message pour demander les règles locales au SPDF.
$C_{SPDF_{LOCAL-RULES}}$	C_6	Coût de la création du message contenant les règles locales.
$C_{RACF_{ANALYSE}}$	C_7	Coût de l'analyse du profil ou la demande de mise à jour avec les règles locales.
$C_{RACF_{RESYNC}}$	C_9	Coût de la création du message pour la re-synchronisation.
$C_{A-RACF_{CONFIG}}$	C_{11}	Coût de la création du message pour la configuration du RCEF ou du BGF.
$C_{BGF_{CONFIG}}$	C_{12}	Coût de la configuration du BGF.
$C_{RCEF_{CONFIG}}$	C_{13}	Coût de la configuration du RCEF.
$C_{A-RACF_{CONFIG}}$	C_{16}	Coût de la configuration du A-RACF.
$C_{NACF_{CONFIG}}$	C_{18}	Coût de la configuration du NACF.
$C_{UAAF_{CONFIG}}$	C_{19}	Coût de la configuration du UAAF.
$C_{CLF_{ASK-CONFIG}}$	C_{20}	Coût de la création d'un message de configuration.
$C_{CLF_{CONFIG}}$	C_{23}	Coût de la configuration du CLF.
$C_{MN_{ASKCONFIG}}$	C_{24}	Coût de la création du message de mise à jour du mobile.
$C_{MN_{CONFIG}}$	C_{25}	Coût de la configuration du mobile.

$C_{CLF_{PROXY}}$	C_{29}	Coût de la création du message pour configurer le proxy CLF.
$C_{CLF_{PROXY-UPDATE}}$	C_{30}	Coût de la configuration du proxy CLF.
$C_{PDBF-RACF}$	C_2	Coût de transport entre le PDBF et le RACF du même domaine.
$C_{RACF-I-RACF}$	C_3	Coût de transport entre le RACF et le I-RACF du même domaine.
$C_{V-I-RACS-H-I-RACS}$	C_4	Coût de transport entre le V-I-RACS du domaine visité et le H-I-RACS du domaine d'attache.
$C_{RACF-SPDF}$	C_8	Coût de transport entre le RACF et le SPDF du même domaine.
$C_{RACF-A-RACF}$	C_{10}	Coût de transport entre le RACF et le A-RACF du même domaine.
$C_{A-RACF-BGF}$	C_{14}	Coût de transport entre le A-RACF et le BGF du même domaine.
$C_{A-RACF-RCEF}$	C_{15}	Coût de transport entre le A-RACF et le RCEF du même domaine.
$C_{RACF-CLF}$	C_{17}	Coût de transport entre le RACF et le CLF du même domaine.
$C_{CLF-NACF}$	C_{21}	Coût de transport entre le CLF et le NACF du même domaine.
$C_{CLF-UAAF}$	C_{22}	Coût de transport entre le CLF et le UAAF du même domaine.
$C_{AMF-UAAF}$	C_{26}	Coût de transport entre l'AMF et le UAAF du même domaine.
$C_{AMF-NACF}$	C_{27}	Coût de transport entre l'AMF et le NACF du même domaine.
C_{AMF-MN}	C_{28}	Coût de transport entre l'AMF et le MN du même domaine.
$C_{CLF-I-NASS}$	C_{31}	Coût de transport entre le CLF et le I-NASS du même domaine.
$C_{V-I-NASS-H-I-NASS}$	C_{32}	Coût de transport entre le V-I-NASS du domaine visité et le H-I-NASS du domaine d'attache.

La Figure 4.30 montre le diagramme de séquence pour le processus de mise à jour initié par le PDBF (un type d'initiation de mise à jour) du réseau d'attache.

Le processus engendre donc le modèle suivant :

$$C_1 + C_2 + C_3 + C_4 + C_3 + C_5 + C_8 + C_6 + C_8 + C_7 +$$

$$C_9 + C_3 + C_4 + C_3 + C_7 + C_9 + C_3 + C_4 + C_3 + C_7 +$$

$$C_9 + C_{10} + C_{11} + C_{14} + C_2 + C_{11} + C_{15} + C_{13} + C_{14} +$$

$$C_{15} + C_{16} + C_{10} + C_9 + C_{17} + C_{20} + C_{21} + C_{18} + C_{20} +$$

$$C_{22} + C_{19} + C_{21} + C_{22} + C_{23} + C_{24} + C_{27} + C_{28} + C_{25} +$$

$$C_{28} + C_{27} + C_{24} + C_{26} + C_{28} + C_{25} + C_{28} + C_{26} + C_{29} +$$

$$C_{31} + C_{32} + C_{31} + C_{30} + C_{31} + C_{32} + C_{31}$$

$$= C_1 + 2 * C_2 + 6 * C_3 + 3 * C_4 + C_5 + C_6 3 * C_7 + 2 * C_8 +$$

$$4 * C_9 + 2 * C_{10} + 2 * C_{11} + C_{13} + 2 * C_{14} + 2 * C_{15} + C_{16} +$$

$$C_{17} + C_{18} + C_{19} + 2 * C_{20} + 2 * C_{21} + 2 * C_{22} + C_{23} + 2 * C_{24} +$$

$$2 * C_{25} + 2 * C_{26} + 2 * C_{27} + 4 * C_{28} + C_{29} + C_{30} + 4 * C_{31} + 2 * C_{32}$$

Nous faisons l'hypothèse simplificatrice suivante pour rendre plus facilement analysable le modèle :

- les temps de traitement ou de création des requêtes sont au maximum de 1 ms (réaliste avec les vitesses des processeurs actuels).

Nous avons aussi effectué les simplifications de variables suivantes :

- $C_{INTER-DOMAINES} = C_4 = C_{32}$;
- $C_{INTRA-DOMAINE} = C_2 = C_3 = C_{31}$;
- $C_{INTRA-RACS} = C_8 = C_{10} = C_{14} = C_{15} = C_{17}$;
- $C_{INTRA-NASS} = C_{21} = C_{22} = C_{26} = C_{27}$;
- $C_{ACCES} = C_{28}$.

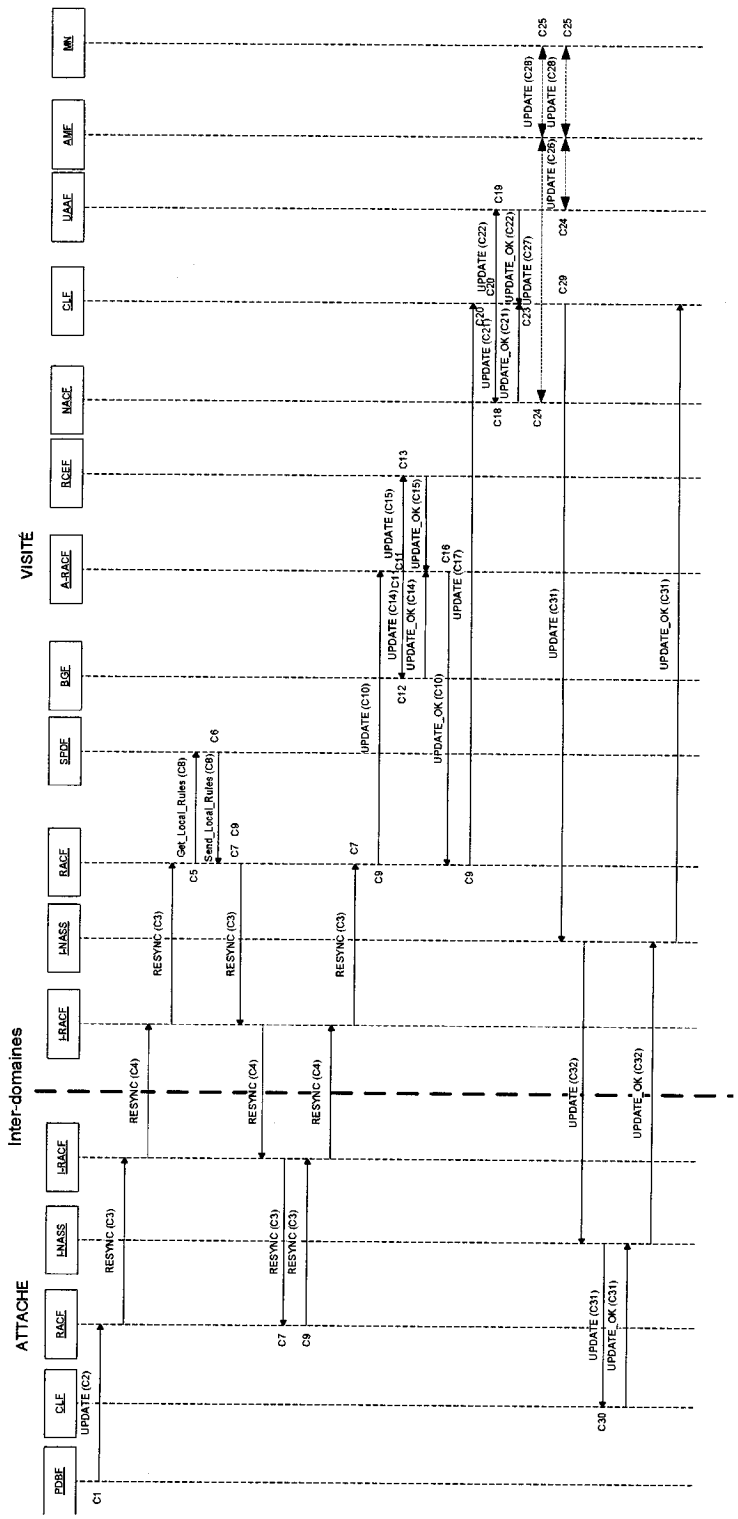

FIGURE 4.30 Nouveau scénario de mise à jour

Avec les simplifications et les hypothèses simplificatrices précédentes le modèles sans devient :

$$C_{total} = 1ms + 8 * C_{INTRA-DOMAINE} + 3 * C_{INTER-DOMAINES} + 1ms + 1ms + 3ms +$$
$$2 * C_{INTRA-RACS} + 4ms + 2 * C_{INTRA-RACS} + 2ms + 1ms + 4 * C_{INTRA-RACS} + 1ms +$$
$$C_{INTRA-RACS} + 1ms + 1ms + 2ms + 4 * C_{INTRA-NASS} + 1ms + 2ms + 2ms +$$
$$4 * C_{INTRA-NASS} + 4 * C_{ACCES} + 1ms + 1ms + 4 * C_{INTRA-DOMAINE} +$$
$$2 * C_{INTER-DOMAINES}$$

$$C_{total} = 4 * C_{ACCES} + 12 * C_{INTRA-DOMAINE} + 5 * C_{INTER-DOMAINES} +$$
$$9 * C_{INTRA-RACS} + 8 * C_{INTRA-NASS} + 25ms$$

Puisque le modèle se réduit maintenant à 5 variables, nous allons faire 5 graphiques avec quatre variables fixes et une variable non-fixe dans chacun d'eux. Cela revient à faire une étude de type *un facteur à la fois* et cela permet de déterminer l'importance de chacune des variables. Cependant, tous les cas ne seront pas explorés, comme le montrent les Figures 4.31 à 4.35.

Le premier graphique représente le coût total en temps versus C_{ACCES}. La liste suivante donne les variables fixées ainsi que leur valeur :

- $C_{INTRA-DOMAINE} = 10$ ms ;
- $C_{INTER-DOMAINES} = 50$ ms ;
- $C_{INTRA-RACS} = 5$ ms ;
- $C_{INTRA-NASS} = 5$ ms.

La Figure 4.31 montre le premier graphique. Nous y voyons bien l'effet du facteur 4 qui multiplie C_{ACCES} dans le modèle. Ce facteur est l'un des plus petits, car seulement 2 messages (aller-retour) sont nécessaires pour re-négocier le mobile.

Le second graphique représente le coût total en temps versus $C_{INTRA-DOMAINE}$. La liste suivante donne les variables fixées ainsi que leur valeur :

- $C_{ACCES} = 20$ ms ;

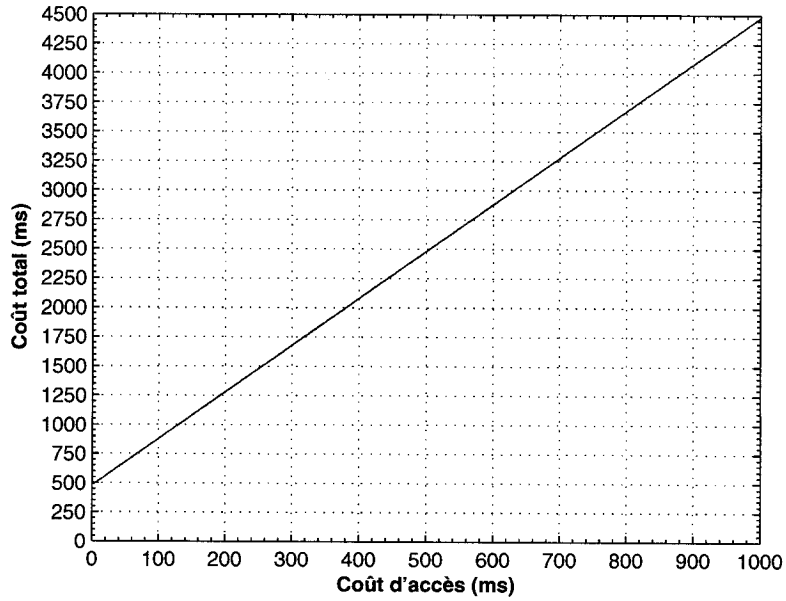

FIGURE 4.31 Coût total versus le C_{ACCES} pour le scénario de mise à jour

- $C_{INTER-DOMAINES} = 50$ ms ;
- $C_{INTRA-RACS} = 5$ ms ;
- $C_{INTRA-NASS} = 5$ ms.

La Figure 4.32 montre le deuxième graphique. Nous y voyons bien l'effet du facteur 12 qui multiplie $C_{INTRA-DOMAINE}$ dans le modèle. Ce facteur est le plus élevé, car nous favorisons la communication intra-domaine par rapport à celle inter-domaines.

Le troisième graphique représente le coût total en temps versus $C_{INTER-DOMAINES}$. La liste suivante donne les variables fixées ainsi que leur valeur :

- $C_{ACCES} = 20$ ms ;
- $C_{INTRA-DOMAINE} = 10$ ms ;
- $C_{INTRA-RACS} = 5$ ms ;
- $C_{INTRA-NASS} = 5$ ms.

La Figure 4.33 montre le troisième graphique. Nous y voyons bien l'effet du facteur 5 qui multiplie $C_{INTER-DOMAINES}$ dans le modèle. Ce type de coût est le plus dispendieux de tous. Nous essayons donc de le limiter, mais le réseau d'attache doit informer le réseau visité d'une mise à jour et vice-versa.

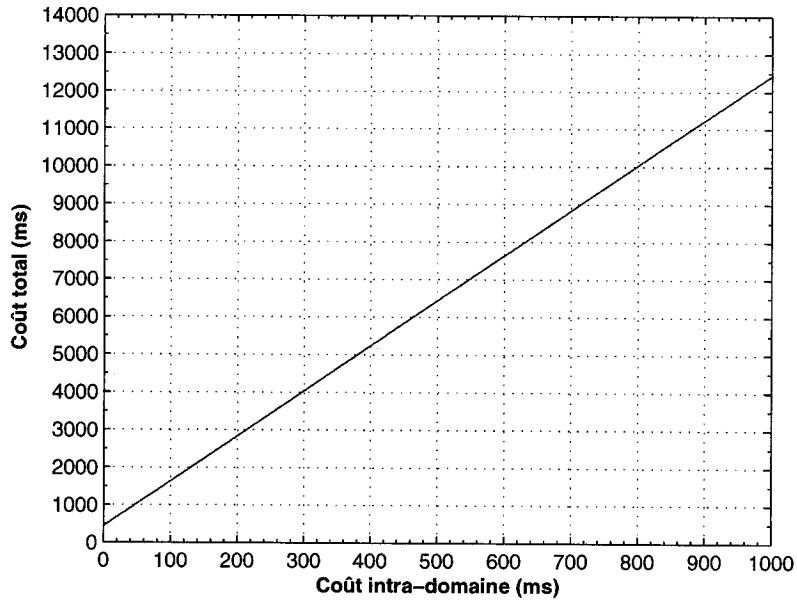

FIGURE 4.32 Coût total versus le $C_{INTRA-DOMAINE}$ pour le scénario de mise à jour

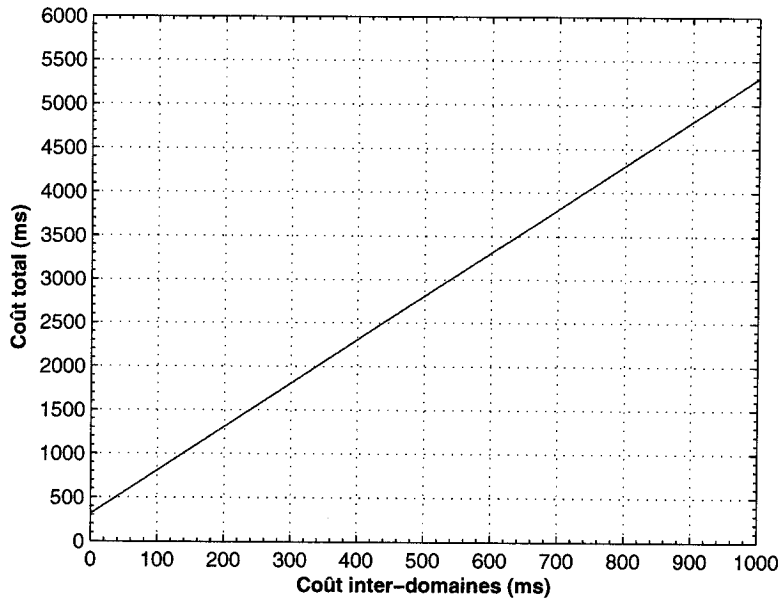

FIGURE 4.33 Coût total versus le $C_{INTER-DOMAINES}$ pour le scénario de mise à jour

Le quatrième graphique représente le coût total en temps versus $C_{INTRA-RACS}$. La liste suivante donne les variables fixées ainsi que leur valeur :

- $C_{ACCES} = 20$ ms ;
- $C_{INTRA-DOMAINE} = 10$ ms ;
- $C_{INTER-DOMAINES} = 50$ ms ;
- $C_{INTRA-NASS} = 5$ ms.

La Figure 4.34 montre le quatrième graphique. Nous y voyons bien l'effet du facteur 9 qui multiplie $C_{INTRA-RACS}$ dans le modèle. Ce facteur est principalement dû à la re-configuration de toutes les parties du RACS lorsque le réseau doit modifier les réservations d'un usager. Ce type de coût est habituellement petit, donc souvent de moindre importance par rapport aux autres.

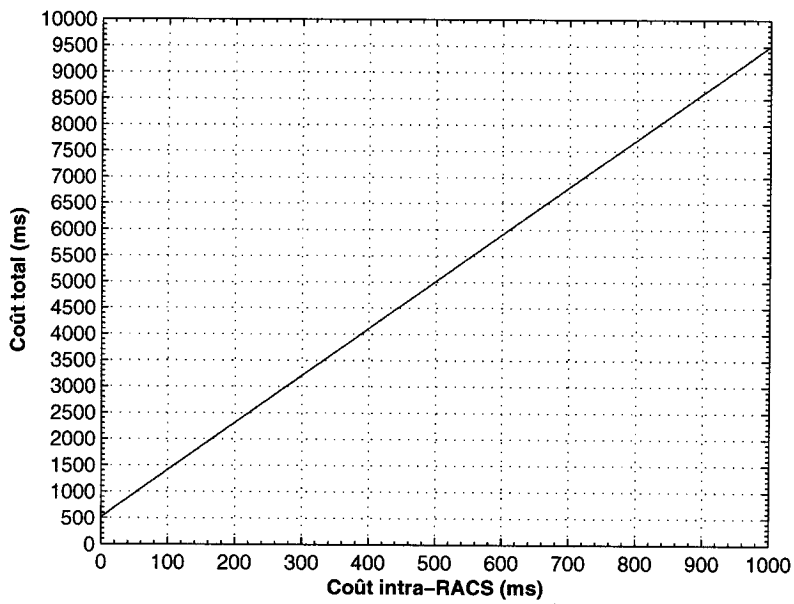

FIGURE 4.34 Coût total versus le $C_{INTRA-RACS}$ pour le scénario de mise à jour

Le cinquième graphique représente le coût total en temps versus $C_{INTRA-NASS}$. La liste suivante donne les variables fixées ainsi que leur valeur :

- $C_{ACCES} = 20$ ms ;
- $C_{INTRA-DOMAINE} = 10$ ms ;
- $C_{INTER-DOMAINES} = 50$ ms ;
- $C_{INTRA-RACS} = 5$ ms.

La Figure 4.35 montre le cinquième graphique. Nous y voyons bien l'effet du facteur 8 qui multiplie $C_{INTRA-NASS}$ dans le modèle. Ce facteur est principalement dû à la re-configuration de toutes les parties du NASS lors d'un besoin de modifier les configurations d'accès d'un usager. Ce type de coût est habituellement petit, donc souvent de moindre importance par rapport aux autres.

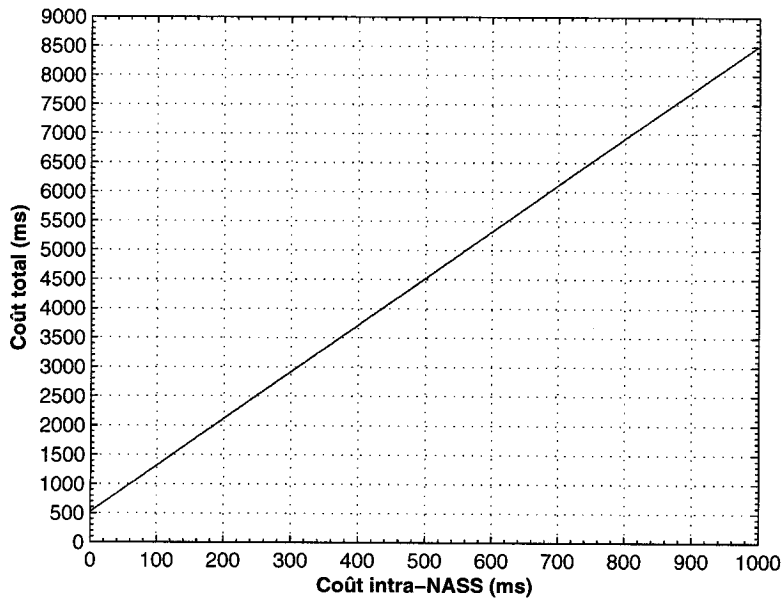

FIGURE 4.35 Coût total versus le $C_{INTRA-NASS}$ pour le scénario de mise à jour

Pour des valeurs normales de coûts (C_{ACCES} = 20 ms, $C_{INTRA-DOMAINE}$ = 10 ms, $C_{INTER-DOMAINES}$ = 50 ms, $C_{INTRA-RACS}$ = 5 ms et $C_{INTRA-NASS}$ = 5 ms), on trouve un coût total de 560 ms pour le modèle. Un délai de 560 ms est très acceptable pour que le réseau d'attache et les réservations du réseau visité soient mis à jour. La re-négociation optionnelle avec le mobile est aussi incluse dans ce coût.

4.3 Volet 3

Dans cette section, nous effectuerons l'analyse de performance du volet 3 de la solution qui a été présentée au chapitre précédent. Le présent volet aborde principalement l'aspect de facturation. Pour l'élaboration des modèles analytiques de ce

volet, nous allons utiliser les coûts suivants :

$C_{RCEF-P-CDCF}$	C_1	Coût de transport entre le RCEF et le P-CDCF dans le même domaine.
$C_{BGF-P-CDCF}$	C_1	Coût de transport entre le BGF et le P-CDCF dans le même domaine.
$C_{I-CDCF-S-CDCF}$	C_3	Coût de transport entre le I-CDCF et le S-CDCF dans le même domaine.
$C_{I-CDCF-P-CDCF}$	C_7	Coût de transport entre le I-CDCF et le P-CDCF dans le même domaine.
$C_{V-I-CDCF-H-I-CDCF}$	C_8	Coût de transport entre le V-I-CDCF et le H-I-CDCF inter-domaines.

$C_{RCEF_{PREPARE}}$	C_4	Coût de la préparation des informations par le RCEF.
$C_{BGF_{PREPARE}}$	C_5	Coût de la préparation des informations par le BGF.
$C_{CDCF_{ANALYSE}}$	C_6	Coût de l'analyse des informations par le CDCF.

Nous dressons une liste commune des coûts afin d'établir une uniformité entre les différents modèles. Nous supposons les coûts symétriques. Il est aussi important de noter que seulement les coûts de traitement et de préparation des requêtes prédominants y sont inclus. Nous avons effectué ces simplifications afin de rendre les modèles plus simples et plus compréhensibles.

4.3.1 Ajout d'informations de facturation dans le profil QdS et contrôle des services

Il a été proposé d'ajouter le type de facturation ainsi que l'intervalle auquel envoyer les informations de facturation. On ajoute donc ces informations au profil QdS et contrôle des services présenté au Tableau 4.2 du volet 1. Le Tableau 4.5 montre le profil modifié. Les champs ajoutés sont les suivants :

a) le type de facturation : supposons 8 bits (le minimum pour être aligné sur des octets) ;

b) l'intervalle d'envoi des informations : supposons 16 bits (de 0 à $2^{16} = 65536$ secondes ou ms).

TABLEAU 4.5 Ajout des informations de facturation dans le profil QdS et contrôle des services

Profil de QdS	
- Classe de service de transport	La classe de service de transport souscrite par l'usager.
- Bande passante souscrite en amont	La quantité maximale de bande passante souscrite par l'usager en amont.
- Bande passante souscrite en aval	La quantité maximale de bande passante souscrite par l'usager en aval.
- Types de flots supportés	Vidéo, audio, data, etc.
- Différents types de flot	Bande passante souscrite en amont
	Bande passante souscrite en aval
	Priorité maximale pour la réservation
	Classe de service de transport (premium, normal, etc.)
	Les Ids des classes d'applications
Configuration initiale des grilles	
- Liste des destinations permises	La liste des adresses de destination par défaut, des ports, des préfixes et des intervalles de ports auquels du trafic peut être envoyé.
- Bande passante par défaut en amont	La quantité maximale de bande passante qui peut être utilisée sans autorisation explicite en amont.
- Bande passante par défaut en aval	La quantité maximale de bande passante qui peut être utilisée sans autorisation explicite en aval.
Configuration initiale du contrôle des services (Optionel)	
ID type de contrôle	Nombre d'argument(s)
Argument 1	Argument 2
...	
...	...
Type de facturation	Facturation en temps réel ou en différé
Intervalle d'envoi des informations	Intervalle de temps entre chaque envoi d'informations de facturation

Cela correspond donc à l'ajout de 24 bits, donc à une augmentation de la taille du profil de QdS et contrôle des services de 3,70% en moyenne.

$$((672bits - 648bits)/648bits) * 100\% = 3,70\%$$

Lorsque le profil a sa taille minimum, l'ajout des informations de facturation augmente la taille des données de 33,33%.

$$((96bits - 72bits)/72bits) * 100\% = 33,33\%$$

Enfin, lorsque le profil a sa taille maximale, l'ajout des informations de facturation augmente la taille des données de 0,03%.

$$((75344bits - 75320bits)/75320bits) * 100\% = 0,03\%$$

Il en résulte donc une influence quasi-négligeable sur la taille du profil puisque la taille des informations ajoutées est petite. Cela aura donc une petite répercussion sur le délai de transmission. Nous supposons que les délais de traitement, de propagation ($distance * 5\mu s/km$) et d'attente (longueur du tampon * % d'utilisation / capacité) ne dépendent pas de la longueur des paquets. Le délai de transmission est donné par la formule suivante :

$$Delai=Longueur/Capacite$$

On suppose des liens ayant des capacités de 1 Mbps (1 000 000 bits/s). Donc, avec l'ajout de 24 bits d'information, la différence de délai est de 24 μs :

$$672bits/1Mbps - 648bits/1Mbps = 24\mu s$$

Nous pouvons donc conclure que cet ajout a peu d'influence sur le délai de transmission. Il est aussi intéressant de noter que si un protocole de type XML était utilisé, il faudrait rajouter la taille des balises dans les calculs. Dans le cas d'un protocole standard (non-XML), des informations sur la longueur des champs variables devraient être rajoutées et donc incluses dans les calculs.

4.3.2 Facturation intra-domaine

Dans cette sous-section, le nouveau processus d'échange des informations de facturation intra-domaine (lorsque l'usager est dans son réseau d'attache) sera analysé. Ce sera fait à l'aide d'un modèle analytique et d'une validation formelle.

La Figure 4.36 montre le diagramme de séquence pour l'échange des informations de facturation intra-domaine.

Nous en déduirons un modèle analytique qui permettra d'analyser ses performances. Nous utiliserons la liste des variables présentée au début du Volet 3.

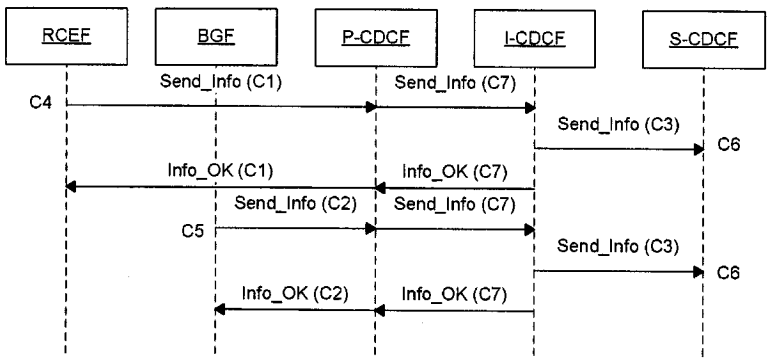

FIGURE 4.36 Scénario de facturation intra-domaine

Le processus du RCEF engendre le modèle suivant :

$$C_4 + C_1 + C_7 + C_3 + C_6 + C_7 + C_1$$

$$= 2 * C_1 + C_3 + C_4 + C_6 + 2 * C_7$$

Le processus du BGF engendre le modèle suivant :

$$C_5 + C_2 + C_7 + C_3 + C_6 + C_7 + C_2$$

$$= 2 * C_2 + C_3 + C_5 + C_6 + 2 * C_7$$

Nous faisons l'hypothèses simplificatrice suivante pour rendre plus facilement comparable les deux modèles :

- les temps de traitement ou de création des requêtes sont au maximum de 1 ms (réaliste avec les vitesses des processeurs actuels).

Nous avons aussi effectué la simplification de variable suivante :

- $C_{INTRA-DOMAINE} = C_1 = C_2 = C_3 = C_7$.

Avec les simplifications et les hypothèses simplificatrices précédentes les modèles deviennent :

$$C_{total-RCEF} = 3 * C_{INTRA-DOMAINE} + 1ms + 1ms + 2 * C_{INTRA-DOMAINE}$$

$$C_{total-RCEF} = 5 * C_{INTRA-DOMAINE} + 2ms$$

$$C_{total-BGF} = 3 * C_{INTRA-DOMAINE} + 1ms + 1ms + 2 * C_{INTRA-DOMAINE}$$

$$C_{total-BGF} = 5 * C_{INTRA-DOMAINE} + 2ms$$

Il est important de noter que les deux modèles sont identiques après les simplifications et les hypothèses. Nous allons donc seulement considérer un des deux ($C_{total-BGF} = C_{total-RCEF} = C_{total}$).

Puisque les modèles se réduisent maintenant à une variable, nous allons seulement faire un graphique.

La Figure 4.37 montre le coût total en temps versus $C_{INTRA-DOMAINE}$. Nous y voyons bien l'effet du facteur 5 qui multiplie $C_{INTRA-DOMAINE}$ dans le modèle.

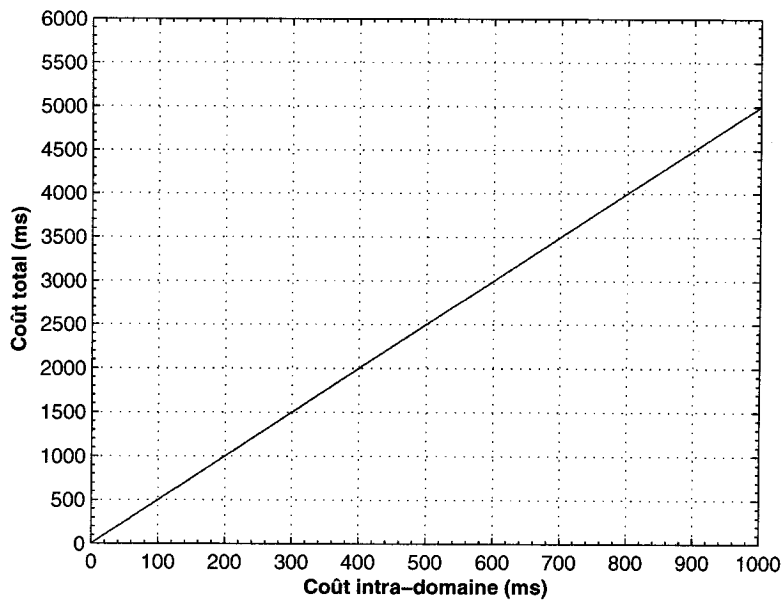

FIGURE 4.37 Coût total versus le $C_{INTRA-DOMAINE}$ pour le scénario de facturation intra-domaine

Pour des valeurs normales des coûts ($C_{INTRA-DOMAINE}$ = 10 ms), on trouve un

coût total de 52 ms pour le modèle. Ce délai est très acceptable pour transmettre les informations de facturation. Il est important de noter que le processus aurait pu être modélisé autrement ; c'est-à-dire, qu'on aurait pu effectuer de l'agrégation sur les différents noeuds intermédiaires (ex : sur le RCEF, sur le BGF, sur le P-CDCF, sur le I-CDCF) pour éviter les flots continuels.

Nous avons ensuite utilisé le logiciel UPPAAL pour effectuer la validation formelle du processus. Plus précisément, nous avons créé un fichier UPPAAL contenant une version du processus d'envoi des informations de facturation intra-domaine. Ce fichier est disponible par le biais du groupe LARIM de l'École Polytechnique de Montréal.

La version réalisée est une version qui correspond plus à une preuve de concept qu'à un modèle complet. En effet, dans ce modèle, il n'y a aucune gestion d'exception. Le but ultime de ce modèle est de vérifier que le processus peut fonctionner sans blocage, et par le fait même dresser une liste des différents noeuds et messages impliqués dans le temps.

La seule propriété temporelle que nous avons testée est celle du blocage.

La propriété de blocage (*A[] not deadlock*) nous permet de vérifier que le protocole ne bloquera jamais. Dans notre cas, la satisfaction de cette propriété nous est suffisante pour prouver que le processus est bien défini, car si l'une des étapes n'avait pas fonctionné, nous serions en blocage.

4.3.3 Facturation inter-domaines

Dans cette sous-section, le nouveau processus d'échange des informations de facturation inter-domaines (lorsque l'usager est en visite dans un autre réseau d'attache) sera analysé. Ce sera fait à l'aide d'un modèle analytique et d'une validation formelle.

La Figure 4.38 montre le diagramme de séquence pour l'échange des informations de facturation inter-domaines.

Nous en déduirons un modèle analytique qui permettra d'analyser ses performances. Nous utiliserons la liste des variables présentée au début du Volet 3.

Le processus du RCEF engendre le modèle suivant :

$$C_4 + C_1 + C_7 + C_7 + C_8 + C_1 + C_3 + C_6 + C_8$$

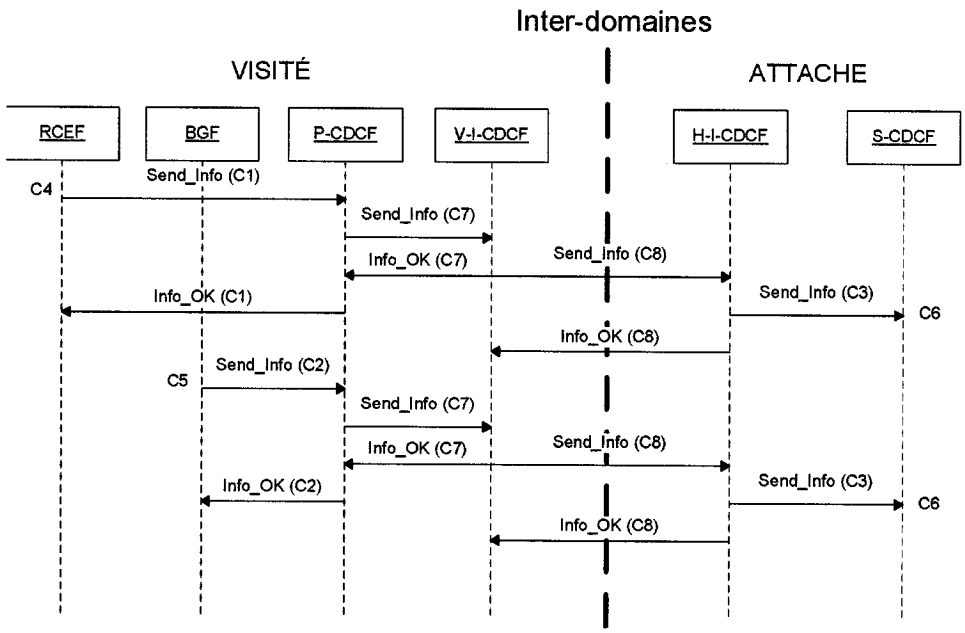

FIGURE 4.38 Scénario de facturation inter-domaine

$$= 2 * C_1 + C_3 + C_4 + C_6 + 2 * C_7 + 2 * C_8$$

Le processus du BGF engendre le modèle suivant :

$$C_5 + C_2 + C_7 + C_7 + C_8 + C_2 + C_3 + C_6 + C_8$$

$$= 2 * C_2 + C_3 + C_5 + C_6 + 2 * C_7 + 2 * C_8$$

Nous faisons l'hypothèse simplificatrice suivante pour rendre plus facilement comparable les deux modèles :

- les temps de traitement ou de création des requêtes sont au maximum de 1 ms (réaliste avec les vitesses des processeurs actuels).

Nous avons aussi effectué les simplifications de variables suivantes :

- $C_{INTER-DOMAINES} = C_8$;
- $C_{INTRA-DOMAINE} = C_1 = C_2 = C_3 = C_7$.

Avec les simplifications et les hypothèses simplificatrices précédentes les modèles deviennent :

$$C_{total-RCEF} = 3 * C_{INTRA-DOMAINE} + 1ms + 1ms + 2 * C_{INTRA-DOMAINE} + 2 * C_{INTER-DOMAINES}$$

$$C_{total-RCEF} = 5 * C_{INTRA-DOMAINE} + 2 * C_{INTER-DOMAINES} + 2ms$$

$$C_{total-BGF} = 3 * C_{INTRA-DOMAINE} + 1ms + 1ms + 2 * C_{INTRA-DOMAINE} + 2 * C_{INTER-DOMAINES}$$

$$C_{total-BGF} = 5 * C_{INTRA-DOMAINE} + 2 * C_{INTER-DOMAINES} + 2ms$$

Il est important de noter que les deux modèles sont identiques après les simplifications et les hypothèses. Nous allons donc seulement considérer un des deux ($C_{total-BGF} = C_{total-RCEF} = C_{total}$).

Puisque les modèles comportent 2 variables, nous allons faire 2 graphiques avec une variable fixe et une variable non-fixe dans chacun d'eux. Cela revient à faire une étude de type *un facteur à la fois* et cela permet de déterminer l'importance de chacune des variables. Cependant, tous les cas ne seront pas explorés. Dans les prochains paragraphes, vous retrouverez les 2 graphiques.

La Figure 4.39 représente le coût total en temps versus $C_{INTRA-DOMAINE}$ avec $C_{INTER-DOMAINES}$ fixé à 50 ms. Nous y voyons bien l'effet du facteur 5 qui multiplie $C_{INTRA-DOMAINE}$ dans le modèle.

La Figure 4.40 représente le coût total en temps versus $C_{INTER-DOMAINES}$ avec $C_{INTRA-DOMAINES}$ fixé à 10 ms. Nous y voyons bien l'effet du facteur 2 qui multiplie $C_{INTRER-DOMAINES}$ dans le modèle.

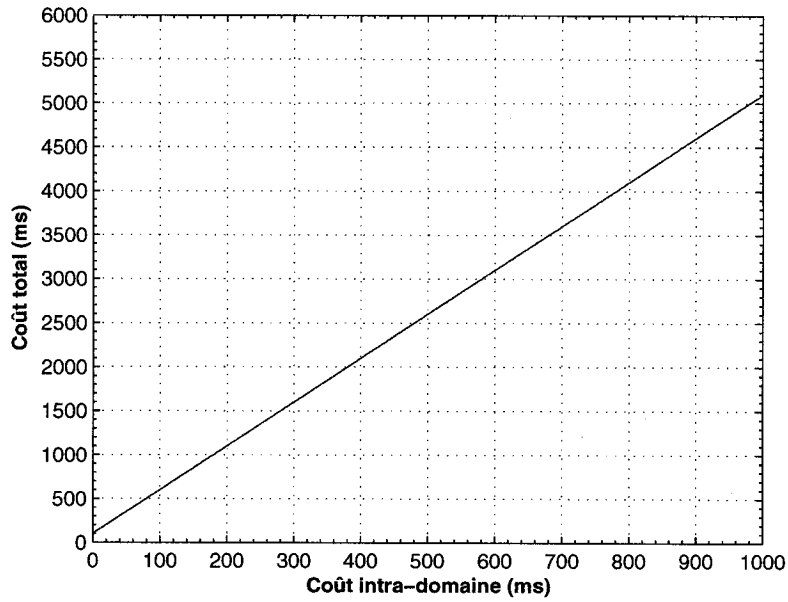

FIGURE 4.39 Coût total versus le $C_{INTRA-DOMAINE}$ pour le scénario de facturation inter-domaines

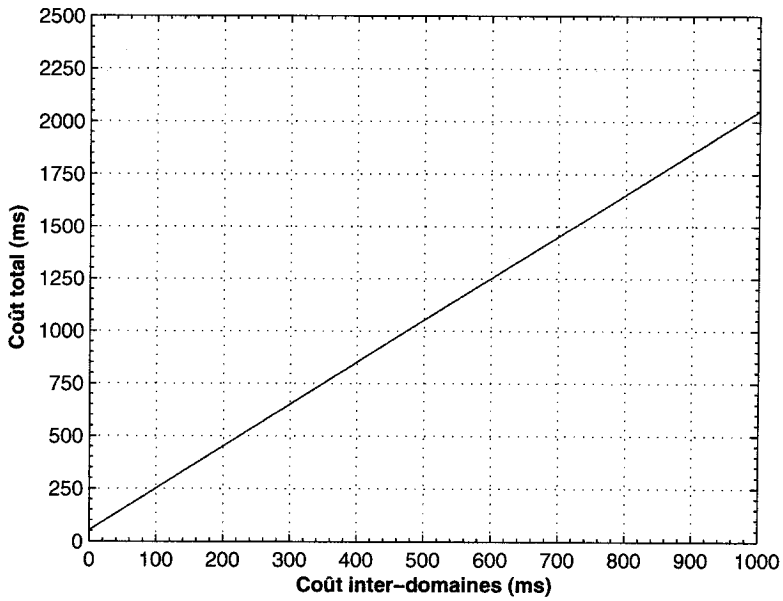

FIGURE 4.40 Coût total versus le $C_{INTER-DOMAINES}$ pour le scénario de facturation inter-domaines

Pour des coûts normaux ($C_{INTRA-DOMAINE}$ = 10 ms et $C_{INTRA-DOMAINE}$ = 50 ms), on trouve un coût total de 152 ms pour le modèle. Ce délai est très acceptable pour transmettre les informations de facturation d'un domaine à un autre. Il est important de noter que le processus aurait pu être modélisé autrement ; c'est-à-dire, qu'on aurait pu effectuer de l'agrégation sur les différents noeuds intermédiaires (ex : sur le RCEF, sur le BGF, sur le P-CDCF, sur le I-CDCF) pour éviter les flots continuels.

Nous avons ensuite utilisé le logiciel UPPAAL pour effectuer la validation formelle du processus. Plus précisément, nous avons créé un fichier UPPAAL contenant une version du processus d'envoi des informations de facturation inter-domaine. Ce fichier est disponible par le biais du groupe LARIM de l'École Polytechnique de Montréal.

La version réalisée est une version qui correspond plus à une preuve de concept qu'à un modèle complet. En effet, dans ce modèle, il y a aucune gestion d'exception. Le but ultime de ce modèle est de vérifier que le processus peut fonctionner sans blocage, et par le fait même dresser une liste des différents noeuds et messages impliqués dans le temps.

La seule propriété temporelle que nous avons testée est celle de blocage.

La propriété de blocage (*A[] not deadlock*) nous permet de vérifier que le protocole ne bloquera jamais. Dans notre cas, la satisfaction de cette propriété nous est suffisante pour prouver que le processus est bien défini, car si l'une des étapes n'avait pas fonctionné, nous serions en blocage.

4.3.4 Modèle combiné

Dans cette section nous allons comparer les délais moyens des 2 scénarios de facturation. Nous allons aussi tracer le graphique résultant de la combinaison des deux modèles.

Le Tableau 4.6 montre les délais de chacun des scénarios. Voici la description sommaire de chacun des scénario :

1. l'usager est dans son réseau d'attache ;
2. l'usager est dans un réseau visité.

Il est intéressant de noter que la seule différence entre les deux scénarios est le délai inter-domaines aller-retour (2*$C_{INTER-DOMAINES}$ = 100 ms).

TABLEAU 4.6 Comparaison des délais moyen des 4 scénarios

Scénario	Délai moyen
1	52 ms
2	152 ms

Nous fixons ensuite des probabilités pour chacun des scénarios afin de tracer un graphique cumulatif. Voici les probabilités que nous allons utiliser :

- scénario 1 : 0,70 ;
- scénario 2 : 0,30.

Nous avons attribué une forte probabilité d'être dans notre réseau d'attache, car nous croyons que c'est le principal patron d'utilisation des réseaux cellulaires. Nous avons ensuite assigné au scénario 2 la probabilité restante $(1 - 0,70 = 0,30$.

Voici le modèle combiné :

$$0,7 * (5 * C_{INTRA-DOMAINE} + 2ms) + 0,3 * (5 * C_{INTRA-DOMAINE} +$$

$$2 * C_{INTER-DOMAINES} + 2ms)$$

Puisque le modèle comporte 2 variables, nous allons faire 2 graphiques avec une variable fixe et une variable non-fixe dans chacun d'eux. Cela revient à faire une étude de type *un facteur à la fois* et cela permet de déterminer l'importance de chacune des variables. Cependant, tous les cas ne seront pas explorés, comme le montrent les Figures 4.41 et 4.42.

La Figure 4.41 représente le coût total en temps versus $C_{INTRA-DOMAINE}$ avec $C_{INTER-DOMAINES}$ fixé à 50 ms. Nous y voyons bien l'effet du facteur 5 $(0,7 * 5 + 0,3 * 5)$ qui multiplie $C_{INTRA-DOMAINE}$ dans le modèle.

La Figure 4.42 représente le coût total en temps versus $C_{INTER-DOMAINES}$ avec $C_{INTRA-DOMAINES}$ fixé à 10 ms. Nous voyons la faiblesse de la pente causée par le facteur 0,6 $(2 * 0,3)$ qui multiplie $C_{INTRER-DOMAINES}$ dans le modèle.

Pour des valeurs normales de coûts, c'est-à-dire $C_{INTRA-DOMAINE} = 10$ ms et $C_{INTRA-DOMAINE} = 50$ ms, on trouve un coût total de 82 ms pour le modèle. Ce délai est très acceptable pour transmettre les informations de facturation d'un domaine (30% du temps) à un autre ou dans le même domaine (70% du temps).

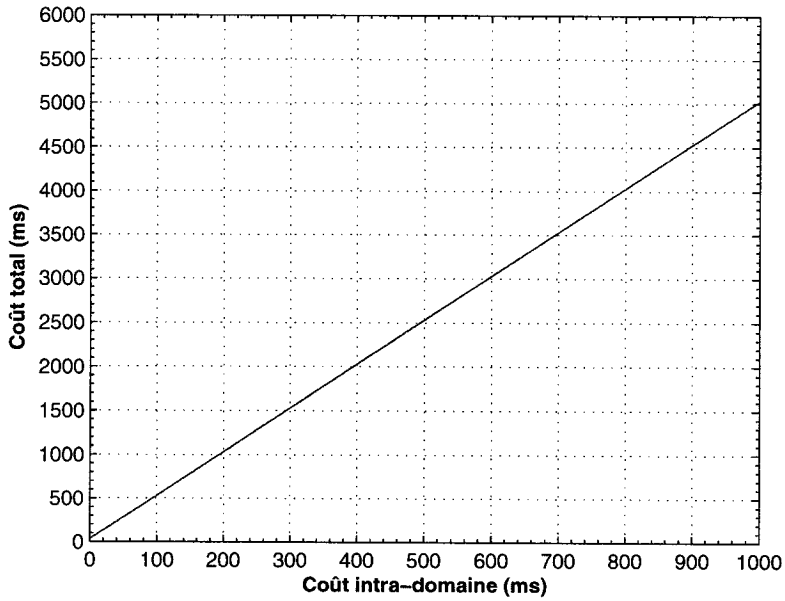

FIGURE 4.41 Coût total combiné versus le $C_{INTRA-DOMAINE}$ pour le modèle de facturation combiné

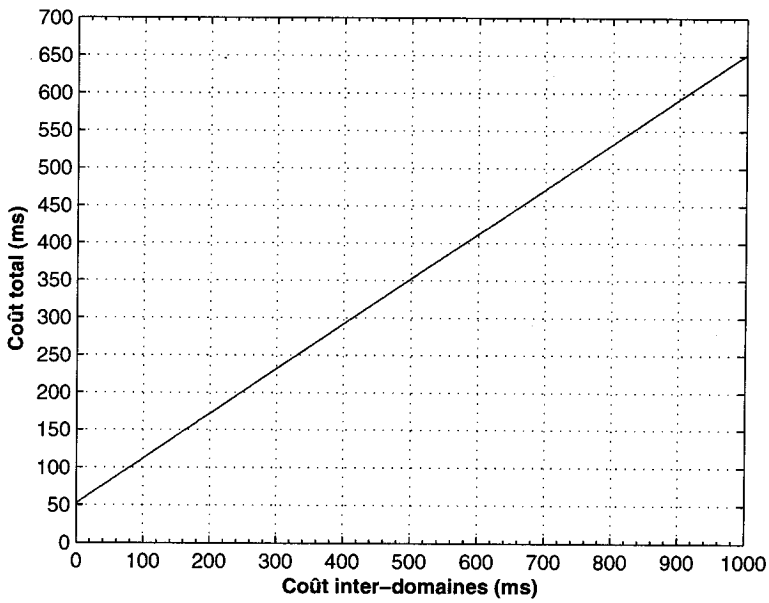

FIGURE 4.42 Coût total combiné versus le $C_{INTER-DOMAINES}$ pour le modèle de facturation combiné

Ainsi s'achève notre analyse de performance. Nous avons confirmé et prouvé que nos modifications de l'architecture et nos nouveaux processus permettaient à un opérateur de contrôler adéquatement les services, la QdS et la facturation d'un usager qui utilise ou non un de ses réseaux d'accès. Nous avons quantifié et analysé les délais supplémentaires générés par ces processus et modifications, et nous en sommes venus à la conclusion qu'ils étaient plus qu'acceptables, voir même souhaitables, pour les usagers d'un réseau de prochaine génération.

CHAPITRE 5

CONCLUSION

Dans ce dernier chapitre, nous résumons les travaux réalisés dans le cadre de ce mémoire, pour ensuite exposer les limitations de notre proposition. Enfin, nous proposons quelques avenues de recherches futures possibles.

5.1 Synthèse des travaux

Ce mémoire a abordé un nouvel aspect de recherche qu'est le développement d'une interface intra-domaine et inter-domaines pour gérer les services, la QdS et la facturation d'un usager qui utilise ou non un réseau d'accès appartenant à son fournisseur d'attache. Nous avons défini l'intra-domaine comme le modèle d'affaire que nous connaissons actuellement ; c'est-à-dire celui dans lequel l'opérateur possède le réseau d'accès ainsi que le réseau de contrôle des services. L'inter-domaines a été défini comme deux domaines complètement distincts. L'usager en utilise un comme réseau visité et l'autre comme réseau d'attache où résident ses services (cela peut être ou non un modèle d'affaire de type MVNO). Pour ce mémoire, nous nous sommes basés sur une architecture hautement en évolution qui est celle des réseaux de prochaine génération. Plus précisément, nous avons choisi celle du groupe TISPAN, car elle est en active définition. De plus, le TISPAN sera probablement un des joueurs les plus importants dans le développement des standards pour ce type de réseaux. Dans ce mémoire, nous avons proposé des ajouts ainsi que des modifications à l'architecture du TISPAN. Entre autres, la création du nouveau noeud dans le RACS, nommé le RACF, qui agit comme point de contrôle et de base de données pour sauvegarder l'état des usagers dans son réseau ainsi que ses usagers d'attache en visite dans d'autres réseaux. Pour continuer, nous avons créé une interface inter-RACF pour permettre l'échange des informations inter-domaines. Nous avons, par la suite, travaillé sur les protocoles nécessaires pour faire fonctionner les nouvelles possibilités offertes par l'architecture modifiée. Premièrement, nous avons fait des modifications au niveau du profil réseau. Nous entendons par modifications, sa segmentation en

un profil d'accès et un profil de QdS et de contrôle des services. Le profil d'accès sert principalement au NASS pour configurer l'accès de l'usager. Nous y avons ajouté un identifiant pour authentifier l'usager. Nous avons ensuite ajouté dans le profil QdS et contrôle des services, des informations plus étendues pour chaque type de flot afin d'améliorer et de rendre plus complet l'interprétation du profil entre les domaines. Nous avons aussi ajouté des informations pour le contrôle des services. Par exemple, cela permet de définir des contrôles de services du type blocage ou redirection de flots ou d'applications. Ensuite, nous avons analysé la différence sur les délais supplémentaires engendrés par l'ajout des informations dans les profils. Nous avons analysé différents scénarios avec l'aide de modèles analytiques et/ou du logiciel de validation formelle UPPAAL. Plus précisément, nous avons analysé les cas suivants :

1. des scénarios d'échange des profils inter et intra-domaine avec et sans modifications ;
2. des scénarios de réservation de ressources intra-domaine avec et sans modifications ;
3. des scénarios de réservations de ressources inter-domaines avec l'utilisation d'IMS ou non et même avec l'utilisation du serveur d'applications directement dans le réseau visité avec ou sans modifications ;
4. un scénario cumulé des différents scénarios de réservations de ressources intra-domaine et inter-domaines avec ou sans modification ;
5. un scénario de mise à jour des réservations de ressources engendré par une modification du profil de l'usager ;
6. des scénarios pour cumuler et transmettre les informations de facturation intra et inter-domaines avec et sans modifications ;
7. un scénario cumulé pour la facturation intra et inter-domaines.

Les résultats ressortant de ces analyses sont que les mécanismes développés sont bien définis et que les délais supplémentaires engendrés par l'ajout des informations dans les profils sont acceptables. De plus, les coûts supplémentaires engendrés par la modification des mécanismes sont aussi d'un ordre acceptable pour un nouvel usager qui se connecte au réseau (échange du profil), pour une nouvelle réservation engendrée par un usager, pour une mise à jour du profil de l'usager et pour le regroupement et l'échange des informations de facturation. Tous les délais supplémentaires

sont facilement compensables par les nombreuses fonctionnalités ajoutées. Le prochain défi consiste à leur trouver des applications directes pour augmenter l'intérêt des usagers.

5.2 Limitations de la solution proposée

La plus grande limitation dans ce travail réside dans le fait que la plupart des scénarios ont été analysés sans y introduire les mécanismes de gestion des erreurs. Nous avons effectué ce type d'analyse puisque nous avions un trop large éventail de scénarios à parcourir. Nous avons par la suite analysé seulement la propriété temporelle de blocage. En effet, ce mémoire était un projet de défrichage et servira probablement à plusieurs travaux futurs ; c'est-à-dire que chacun des 3 volets de la solution pourrait servir à des projets plus poussés. Il serait intéressant de définir le détail de chacun des messages pour tous les processus. Cependant, le volet 1 de la solution a été analysé plus en détail avec des automates plus complets qui incluaient la gestion des erreurs. Le seul problème avec cette approche a été l'atteinte des limites du logiciel UPPAAL. En résumé, nous avons dépassé la mémoire maximale par processus et nous avons pu seulement utiliser le simulateur pour prouver le bon fonctionnement du modèle complet. De plus, les mécanismes de gestion des erreurs auraient pus être ajoutés au équations des modèles analytiques sous formes de probabilités. Cela a été omis car encore une fois le travail serait devenu trop important pour un seul projet. Un autre aspect négligé dans ce mémoire, dû davantage au fait que nous avions trop de sujets à traiter que par le manque d'intérêt, est l'analyse des aspects de micro-mobilité. Il était cependant plus urgent de définir les mécanismes de base et de macro-mobilité avant de s'attaquer aux aspects spécifiques de la mobilité rapide (optimisée). Nous n'avons pas non plus défini comment répartir l'implémentation du contrôle des services entre les noeuds AES et BES du réseau TISPAN. Il est cependant possible que chaque implémentation de ce type de réseau séparera d'une manière différente la gestion des types de contrôle. Pour les aspects de facturation, il serait intéressant de définir différents niveaux d'agrégation ainsi que des mécanismes qui dépendent du profil de l'usager et/ou du règles du réseau local ou distant.

5.3 Améliorations futures

Cette section, avec laquelle nous allons conclure ce mémoire, présente d'éventuelles pistes de recherche. Elles découlent directement des différentes limitations de la solution proposée. Pour commencer, il serait intéressant de reprendre chacun des volets de la solution, de les définir plus en détail et d'y ajouter les les mécanismes de gestion des erreurs et les aspects de micro-mobilité dans les simulations de la validation formelle et dans les équations des modèles analytiques. Nous entendons par micro-mobilité, des mécanismes qui empêchent la re-synchronisation complète du profil de l'usager pour seulement un changement d'AES ou de BES. Une piste possible serait peut-être de se servir des pointeurs de redirection. Par contre, lorsque l'usager change de domaine, le mécanisme de synchronisation complet devra être à nouveau exécuté. Par la suite, on devrait analyser le processus complet de modifications des différents profils découlant de la modifications du profil de services par l'usager. En effet, les profils d'accès et de QdS et de contrôle des services devraient être automatiquement mis à jour en fonction des modifications faites par l'usager ou une autre personne au profil des services. Pour terminer, on pourrait aborder la division du RACS pour chaque section d'un réseau (Accès, Agrégation, coeur, dorsale, etc.) et définir des mécanismes de communication entre les différents RACS.

BIBLIOGRAPHIE

3GPP (2005a). *3GPP TS 23.002 V7.0.0 3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Network architecture (Release 7).* 3GPP.

3GPP (2005b). *3GPP TS 23.228 V7.2.0 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 7).* 3GPP.

BLAKE, S., BLACK, D., CARLSON, M., DAVIES, E., WANG, Z. et WEISS, W. (1998). *RFC2475 : An Architecture for Differentiated Services.* IETF. Status : INFORMATIONAL.

BOURAS, C. et STAMOS, K. (2005). Examining the Benefits of a Hybrid Distributed Architecture for Bandwidth Brokers. *IPCCC2005.*

COCHENNEC, J.-Y. (2002). Activities on Next-Generation Networks Under Global Information Infrastructure in ITU-T. *IEEE Communications Magazine.*

GHYS, F. et VAARANIEMI, A. (2002). Component-Based Charging in a Next-Generation Multimedia Network. *WTC2002.*

ITU-T (2004a). *Y. 2011, General principles and general reference model for next generation networks.* ITU-T.

ITU-T (2004b). *Y.2001, General overview of NGN.* ITU-T.

JOHNSON, D., PERKINS, C. et ARKKO, J. (2004). *RFC3775 : Mobility Support in IPv6.* IETF. Status : STANDARDS TRACK.

KOUCHERYAVY, Y., VASILIEV, A., SOLOVIEV, S. et KOUCHERYAVY, A. (2006). The Public Packet-Switched Network with Guaranteed QoS Based on DiffServ Domains Hierarchy. *ICACT2006.*

KRISHNAMURTHY, A., QIAN, L., WANG, Y., DAUCHY, P. et CONTE, A. (2005). A New Coordinated Scheduling Algorithm in Distributed Bandwidth Broker QoS Architecture. *ICC2005.*

MSF (2005a). *MSF-ARCH-002.00-FINAL Bandwidth Management in Next Generation Packet Networks.* MSF.

MSF (2005b). *MSF-TR-ARCH-005-FINAL MSF Release 2 Architecture.* MSF.

NSIS (2005). *Next Steps in Signaling.* NSIS. URL : http ://www.ietf.org/html.charters/nsis-charter.html.

OPERAX (2005). *A ubiquitous network resource control plane for end-to-end QoS ; Technical White Paper.* Operax.

OUELLETTE, S. (2006). Routage et gestion de la Qualité de Service des flots de données temps-réel dans les réseaux IPv6.

PACKETCABLE (2005a). *PKT-SP-MM-I03-051221 Multimedia Specification.* PacketCable.

PACKETCABLE (2005b). *PKT-TR-ARCH1.5-V01-050128 Architecture Framework Technical Report.* PacketCable.

QUOTIDIEN (2005). *Statistiques des télécommunications.* Gouvernement du Canada. URL : http ://www.statcan.ca/Daily/Francais/051004/q051004a.htm.

SOLIMAN, H., CATELLUCCIA, C., EL MALKI, K. et BELLIER, L. (2005). *RFC4140 : Hierarchical Mobile IPv6 mobility management (HMIPv6).* IETF. Status : EXPERIMENTAL.

TISPAN (2005a). *ETSI ES 282 001 v1.1.1 Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN) NGN Functional Architecture Release 1.* ETSI.

TISPAN (2005b). *ETSI ES 282 003 v1.6.8 Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN) Resource and Admission Control Subsystem (RACS) Functional Architecture.* ETSI.

TISPAN (2005c). *ETSI ES 282 004 v1.1.0 NGN Functional Architecture ; Network Attachment Subsystem ; Release 1.* ETSI.

TISPAN (2005d). *ETSI ES 282 007 v1.2.6 Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN) IP Multimedia Subsystem (IMS) Functional Architecture.* ETSI.

XU, S. et XU, B. (2005). A fair admission control scheme for multimedia wireless network. *Wireless Communications, Networking and Mobile Computing, 2005.*